Massimo comune divisore, equazioni diofantee, congruenze

Mihaela Bădescu

Questa nota richiede la conoscenza della relazione di divisibilità e delle nozioni di numero primo, numero irriducibile e di elemento invertibile. Le notazioni sono quelle usuali. In particolare denotiamo con:

1. $\mathbb{N}$ – l'insieme dei numeri naturali $\{0, 1, 2, 3, \ldots\}$, $\mathbb{N}^* = \{1, 2, 3, \ldots\}$,
2. $\mathbb{Z}$ – l'insieme dei numeri interi $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$, $\mathbb{Z}^* = \{\pm 1, \pm 2, \pm 3, \ldots\} = \mathbb{Z} \setminus \{0\}$,
3. $\mathbb{Q}$ – l'insieme dei numeri razionali,
4. $\mathbb{R}$ – l'insieme dei numeri reali,
5. $\mathbb{C}$ – l'insieme dei numeri complessi.

I. Massimo comune divisore

Definizione 1. *Siano $a, b \in \mathbb{Z}$ due numeri interi, $a \neq 0$. Si dice che a divide b, e si scrive $a|b$, se esiste un numero intero c tale che $a \cdot c = b$. D'ora innanzi, ogni volta quando diciamo che a divide b, cioè $a|b$, sottoindiamo che $a \neq 0$ quando questa cosa non sarà fatta esplicita.*

Definizione 2. *Un numero intero $p \neq 0, 1, -1$ si chiama* numero primo *se e solo se ogni volta che p divide un prodotto di numeri interi, divide almeno uno dei fattori, cioè*

$$p \in \mathbb{Z} \setminus \{0, 1, -1\} \text{ è primo } \iff [\, p|(a \cdot b) \;\Rightarrow\; p|a \;\text{ oppure }\; p|b\,].$$

Definizione 3. *Un numero intero p, $p \neq 0, +1, -1$ si chiama* irriducibile *se e solo se dalla relazione $p = a \cdot b$, con $a, b \in \mathbb{Z}$, segue $a = \pm 1$ oppure $b = \pm 1$.*

È ben noto che un numero intero $p \neq 0, +1, -1$ è primo se e solo se è irriducibile.

Definizione 4. *Siano a e b due numeri interi, non tutti e due nulli. Un numero intero d si chiama il massimo comune divisore di a e b, denotato con $d = (a, b)$, se soddisfa le seguenti condizioni:*

(1) *d è divisore comune di a e b, cioè $d|a$ e $d|b$,*

(2) *Ogni divisore comune $d' \in \mathbb{Z}$ di a e b divide d, cioè se $d'|a$ e $d'|b$ allora $d'|d$.*

Questa definizione usa solo la relazione di divisibilità, senza ricorrere alla relazione di ordine su $\mathbb{Z}$. Perciò la definizione rimane valida nell'anello dei polinomi (a coefficienti numeri interi, razionali, reali o complessi), e, più generalmente, in ogni anello senza divisori di zero.

Se $a, b \in \mathbb{N}^*$ e $a|b$ allora $a \leq b$. Infatti, la condizione $a|b$ significa che esiste $c \in \mathbb{N}^*$ tale che $a \cdot c = b$. Moltiplicando per a la disuguaglianza $1 \leq c$ si ottiene $a \leq a \cdot c = b$, ossia $a \leq b$.

Definizione 5. *In ogni anello A (ed in particolare nell'anello dei numeri interi $\mathbb{Z}$) un elemento a si chiama* invertibile *se esiste $b \in A$ tale che $a \cdot b = b \cdot a = 1$, dove 1 è l'elemento neutro di A rispetto alla moltiplicazione.*

Per esempio, l'insieme degli elementi invertibili del anello $\mathbb{Z}$ è $U(\mathbb{Z}) = \{-1, +1\}$. l'insieme degli elementi invertibili dell'anello degli interi di Gauss

$$\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$$

è $U(\mathbb{Z}[i]) = \{+1, -1, +i, -i\}$. Infatti, osserviano innanzitutto che $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$ e $i \cdot (-i) = 1$, da cui segue che $+1$, -1, $+i$ e $-i$ sono elementi invertibili in $\mathbb{Z}[i]$. Viceversa, sia $z = a + ib \in \mathbb{Z}[i]$ invertibile (con $a, b \in \mathbb{Z}$). Dalla definizione risulta che esiste $w = c + id \in \mathbb{Z}[i]$ (con $c, d \in \mathbb{Z}$) tale che $z \cdot w = 1$. Considerando il modulo di un numero complesso, otteniamo $|z \cdot w| = 1 \iff |z|^2 \cdot |w|^2 = 1$, e tenendo conto che $|z|^2$, $|w|^2$ sono numeri naturali, ne segue $|z|^2 = 1 \iff a^2 + b^2 = 1 \iff [a = \pm 1 \text{ e } b = 0]$, ossia $[a = 0 \text{ e } b = \pm 1] \iff z = 1$, $z = -1$, $z = i$, oppure $z = -i$.

In un modo simile (benchè legermente più complicato) si può dimostrare che gli elementi invertibili dell'anello $\mathbb{Z}[\sqrt{2}] = \{a + b \cdot \sqrt{2} | a, b \in \mathbb{Z}\}$ (si verifica facilmente che $\mathbb{Z}[\sqrt{2}]$ è un anello) sono

$$U(\mathbb{Z}[\sqrt{2}]) = \{\pm 1, \pm(1 + \sqrt{2})^n, \pm(1 - \sqrt{2})^n \mid n \in \mathbb{N}^*\}.$$

Se $a, b \in \mathbb{Z}$, con $a \neq 0$, tali che $a|b$ allora si ha anche $-a|b$. Infatti $a|b \iff$ esiste $c \in \mathbb{Z}$ tale che$ac = b \implies (-a) \cdot (-c) = b \iff -a|b$. Di conseguenza, se $d \in \mathbb{Z}$ soddisfa le condizioni della definizione del massimo comune divisore, risulta che anche $-d$ soddisfa le stesse condizioni.

m

Proposizione 1. *La relazione di divisibilità ha le seguenti proprietà:*

1) *Riflessività: per ogni $a \in \mathbb{Z}^*$,allora $a|a$,*

2) *Antisimmetria: se $a, b, \in \mathbb{Z}^*$ tali che $a|b$ e $b|a$, allora $a = \pm b$,*

3) *Tranzitività: se $a, b, c \in \mathbb{Z}$, con $a, b \neq 0$, tali che $a|b$ e $b|c$, allora $a|c$.*

Dimostrazione.

1) Sia $a \in \mathbb{Z}$; possiamo scrivere $a = a \cdot 1$ e allora $a|a$,

2) Dalle condizioni $a|b$ e $b|a$ risulta $a = b \cdot k$ e $b = a \cdot l$, con $k, l \in \mathbb{Z}$. Perciò otteniamo $a = (a \cdot l) \cdot k \implies l \cdot k = 1$, con $l, k \in \mathbb{Z} \implies k = \pm 1 \implies a = \pm b$.

3) Dalle condizioni $a|b$ e $b|c$ risulta $a \cdot k = b$, $b \cdot l = c$, con $k, l \in \mathbb{Z}$. Moltiplicando prima relazione per l otteniamo $a \cdot (k \cdot l) = b \cdot l = c$, e quindi $a|c$. □

Corollario. *Se d e d' sono due massimi comuni divisori di due numeri interi $a, b \in \mathbb{Z}$, non entrambi nulli, allora $d' = \pm d$. In particolare, il massimo comune divisore di a e b è univocamente determinato a meno di un segno.*

Dimostrazione. Dalla definizione segue che $d|d'$ e $d'|d$, da cui, $d' = \pm d$. □

Osservazione. Dal corollario di sopra segue che, senza restringere la generalità, possiamo supporre che il massimo comune divisore di $a, b \in \mathbb{Z}$ (non entrambi 0) è positivo.

Proposizione 2 (Proprietà del massimo comune divisore).

1) *Se $b \neq 0$ allora $(0, b) = b$.*

2) *Se $a, b \in \mathbb{Z}^*$ e $a|b$ allora $(a, b) = a$.*

3) *$((a, b), c) = (a, (b, c))$, per ogni $a, b, c \in \mathbb{Z}^*$.*

4) *$a \cdot (b, c) = (a \cdot b, a \cdot c)$, per ogni $a, b, c \in \mathbb{Z}^*$.*

5) *Se $a, b, c \in \mathbb{Z}^*$ sono tali che $(a, b) = 1$ e $(a, c) = 1$, allora $(a, b \cdot c) = 1$. Inoltre, se a è primo con b e con c, allora a è primo col prodotto $b \cdot c$.*

6) *Se $a, b, c \in \mathbb{Z}^*$ sono tali che $a|(b \cdot c)$ e $(a, b) = 1$, allora $a|c$. In altre parole, se a divide il prodotto $b \cdot c$, e a è primo con b, allora a divide c.*

7) *Se $a, b, c \in \mathbb{Z}^*$ sono tali che $a|c$ e $b|c$ e $(a, b) = 1$, allora $a \cdot b|c$. In altre parole, se due numeri, primi tra di loro, dividono un terzo numero c, allora il loro prodotto divide c.*

8) *Siano $a, b, c \in \mathbb{Z}^*$ e poniamo $d = (a, b)$. Se $a = d \cdot a_1$, $b = d \cdot b_1$, allora $(a_1, b_1) = 1$.*

Dimostrazione. Per quanto detto soppra, senza restringere la generalità, possiamo supporre che tutti i numeri in questione sono numeri naturali.

1) Sia $d = (0, b)$. Da $b|0$ e da $b|b$ risulta $b|d$. Viceversa, per definizione, si ha $d|b$, da cui $d = b$.

2) Dalle condizioni $a|b$ e $a|a$ risulta che a è un divisore comune di a e b, da cui segue che $a|d$. Viceversa, per definizione, abbiamo $d|a$, e quindi $d = a$.

3) Siano $d := ((a, b), c)$ e $d_1 := (a, (b, c))$. Dimostreremo che $d|d_1$ e $d_1|d$ e quindi $d = d_1$. Dalla condizione $d = ((a, b), c)$ risulta $d|(a, b)$, $d|c \implies d|a$, $d|b$, $d|c \implies d|a$, $d|(b, c) \implies d|d_1$. Nello stesso modo si dimostra che $d_1|d$. Risulta $d = d_1$.

4) Siano $d := (b, c)$ e $d_1 := (a \cdot b, a \cdot c)$. Poiché $d|b$ e $d|c$ si ha $(a \cdot d)|(a \cdot b)$ e $(a \cdot d)|(a \cdot c)$, e quindi $(a \cdot d)|d_1$, o ancora, $d_1 = (a \cdot d) \cdot k$. Viceversa, dalle condizioni $d_1|(a \cdot b)$ $d_1|(a \cdot c)$ si ha:

$$a \cdot b = d_1 \cdot x = a \cdot d \cdot k \cdot x, \quad a \cdot c = d_1 \cdot y = a \cdot d \cdot k \cdot y \iff$$

$$b = (d \cdot k) \cdot x, \quad c = (d \cdot k) \cdot y.$$

Ne segue che $d \cdot k$ è il massimo comune divisore di b e c, e quindi $d \cdot k|d$. Perciò $k = 1$. Sostituendo in $d_1 = (a \cdot d) \cdot k$ si ha $d_1 = a \cdot d$.

5) Utilizzando la proprietà 4), si ha

$$1 = (a, b) = (a, b \cdot 1) = (a, b \cdot (a, c)) = (a, (b \cdot a, b \cdot c)) = ((a, b \cdot a), b \cdot c) = (a, b \cdot c),$$

da cui, $(a, b \cdot c) = 1$.

6) Dalla condizione $a|(b \cdot c)$ risulta che esiste $t \in \mathbb{N}$ tale che $b \cdot c = a \cdot t$. Moltiplicando l'uguaglianza $(a, b) = 1$ per c otteniamo

$$c = (a \cdot c, b \cdot c) = (a \cdot c, a \cdot t) = a \cdot (c, t) \implies a|c.$$

7) Le relazioni $a|c$ e $b|c$ implicano $c = a \cdot a_1 = b \cdot b_1$. Moltiplicando per c l'uguaglianza $(a, b) = 1$ otteniamo

$$c = (a \cdot c, b \cdot c) = (a \cdot b \cdot b_1, b \cdot a \cdot a_1) = a \cdot b \cdot (b_1, a_1) \implies (a \cdot b)|c.$$

8) Ponendo $k := (a_1, b_1)$ si ha $a_1 = k \cdot a_2$ e $b_1 = k \cdot b_2$. Sostituendo nelle relazioni dell'ipotesi otteniamo $a = d \cdot k \cdot a_2$, $b = d \cdot k \cdot b_2$. Da cui risulta che $d \cdot k$ è un divisore a e b. Quindi $(d \cdot k)|d \implies k = 1 \implies (a_1, b_1) = 1$.

Esempio. Sia $a = 12$ e $b = 30$. Determiniamo $d = (12, 30)$ usando esclussivamente la definizione del massimo comune divisore. Denotendo con D_n l'insieme dei divisori naturali del numero naturale n, abbiamo $D_{12} = \{1, 2, 3, 4, 6, 12\}$, $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e $D_{12} \bigcap D_{30} = \{1, 2, 3, 6\}$. Da cui troviamo $d = (12, 30) = 6$. Osserviamo che $1|6, 2|6, 3|6, 6|6$.

È chiaro che questo metodo è assai scomodo in prattica, per cui non verrà quasi mai utilizzato. Un modo più comodo per calcolare il massimo comune divisore utilizza la decomposizione dei numeri naturali in fattori primi. Perciò è necessario ricordare il seguente teorema:

Teorema 1 (Il teorema fondamentale dell' aritmetica). *Ogni numero naturale $n \geq 2$ si decompone univocamente (cioè, a meno dell' ordine dei fattori) in prodotto di numeri primi. In altre parole: ogni $n \in \mathbb{N}^*, n \geq 2$ può essere scritto sotto la forma*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_m^{r_m},$$

dove $p_1, p_2, \ldots, p_m$ sono numeri primi a due a due distinti, e $r_1, r_2, \ldots, r_m \in \mathbb{N}^*$.

La decomposizione in fattori primi ci permette di trovare il massimo comune divisore di due numeri naturali a e b come il prodotto dei fattori primi comuni, ciascuno preso solo una volta sola, con il minimo esponente con cui comparre nelle decomposizioni in fattori primi di a e di b.

Esempio. Siano $a = 2^3 \cdot 5 \cdot 17^2$ e $b = 2 \cdot 3 \cdot 17^4 \cdot 31$. Secondo la regola precedente abbiamo $d = (a, b) = 2 \cdot 17^2 = 578$.

È vero però che in alcuni casi la scomposizione a fattori primi di certi numeri è difficile essere determinata, e perciò anche questo metodo di calcolo del massimo comune divisore diventa difficile.

In seguito, descriviamo un procedimento di calcolo del massimo comune divisore di due numeri naturali, che è basato sul teorema di divisione con resto dei numeri interi. Inoltre otteniamo una relazione lineare, a coefficienti interi, fra i due dati numeri e il loro massimo comune divisore.

È utile ricordare il teorema:

Teorema 2 (Il teorema di divisione col resto). *Per ogni due numeri interi a e b, con $b \neq 0$, esistono e sono unici due numeri interi q e r tali che*

$$a = b \cdot q + r \quad \textit{e, inoltre, } \ 0 \leq r < |b|.$$

Il numero q si chiama il quoziente*, e il numero r si chiama il* resto *della divisione di a con b.*

Sottolineamo che la condizione $0 \leq r < |b|$ è essenziale per l'unicità del quoziente q e del resto r. Questo fatto segue dall'oservazione che, per ogni quoziente q fissato si ha $r = a - b \cdot q$. Per esempio, per $a = 43$ e $b = 7$, tra le uguaglianze $43 = 7 \cdot 6 + 1$, $43 = 7 \cdot 5 + 8$, solo la prima rappresenta l'applicazione del teorema di divisione col resto dei numeri 43 e 7, poiché $0 \leq 1 < 7$ e $8 > 7$.

Inoltre, è utile considerare alcuni esempi dell' applicazione del teorema di divisione col resto, per tutte le quattro possibilità dei segni dei numeri a e b.

Per $a = 39$ e $b = 7$ abbiamo $39 = 7 \cdot 5 + 4$,

per $a = 39$ e $b = -7$ abbiamo $39 = -7 \cdot (-5) + 4$,

per $a = -39$ e $b = 7$ abbiamo $-39 = 7 \cdot (-6) + 3$,

e per $a = -39$ e $b = -7$ abbiamo $-39 = -7 \cdot 6 + 3$.

Teorema 3 (L'algoritmo di Euclide). *Per ogni due numeri naturali $a, b \in \mathbb{N}^*$, existe il massimo comune divisore $d = (a, b)$ e d si ottiene come l'ultimo resto non nullo, della successione di divisioni:*

$$a = b \cdot q_1 + r_1, \quad \textit{con} \quad 0 < r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, \quad \textit{con} \quad 0 < r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, \quad \textit{con} \quad 0 < r_3 < r_2$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad \textit{con} \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+1}.$$

Inoltre, $d = (a, b) = r_n = a \cdot k + b \cdot l$, con $k, l \in \mathbb{Z}$. In altre parole, il massimo comune divisore d di a e b è combinazione lineare di a e b a coefficienti numeri interi.

Dimostrazione. L'algoritmo di Euclide consiste in una successione finita di divisioni col resto poiché fra 0 e b esistono un numero finito di numeri naturali, $(b > r_1 > r_2 > r_3 > \ldots > r_n > 0)$. Si comincia con la divisione (con resto) di a per b e si prosegue dividendo sempre il divisore per il resto, finché il resto non diventerà nullo. In effetti dimostreremo che l'ultimo resto non nullo r_n è massimo comune divisore $d = (a, b)$.

Nella dimostrazione useremo più volte la seguente semplice proprietà: se un numero intero a divide due numeri interi b e c, allora a divide ogni combinazione lineare su $\mathbb{Z}$ di b e c, cioè $a|(b \cdot k + c \cdot l)$ per ogni $k, l \in \mathbb{Z}$.

Dalle relazioni precedenti (dall' ultima verso la prima) otteniamo:

$$r_n | r_{n-1}$$

,

$$r_n | r_{n-1} \text{ e } r_n | r_n \implies r_n | r_{n-2}$$
$$r_n | r_{n-2} \text{ e } r_n | r_{n-1} \implies r_n | r_{n-3}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_n | r_2 \text{ e } r_n | r_1 \implies r_n |$$
$$r_n | r_1 \text{ e } r_n | b \implies r_n | a.$$

Quindi r_n è un divisore comune di a e b.

Sia ora d' un altro divizore comune di a e b. Considerando le medesime relazioni dell'enunciato (questa volta dalla prima verso l'ultima) troviamo:

$$d' | a,\ d' | b \implies d' | r_1 \implies d' | r_2 \implies d' | r_3 \implies \ldots \implies d' | r_n.$$

In questo modo abbiamo dimostrato che $r_n = d$. Inoltre, dalla dimostrazione segue anche che, se $a = b \cdot q + r$, allora il massimo comune divisore di a e b coincide con il massimo comune divisore di b e r, cioè $d = (a, b) = (b, r)$.

Ora, per dimostrare che d è combinazione lineare di a e b a coefficienti in $\mathbb{Z}$, si separano i resti in un membro e si ottiene:

$$r_1 = a - b \cdot q_1$$
$$r_2 = b - r_1 \cdot q_1$$
$$r_3 = r_1 - r_2 \cdot q_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$$
$$r_n = r_{n-2} - r_{n-1} \cdot q_n.$$

Sostituendo i resti dal basso in alto, otteniamo successivamente:

$$r_n = r_{n-2} - r_{n-1} \cdot q_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n = r_{n-2} \cdot (1 + q_{n-1} \cdot q_n) - r_{n-3} \cdot q_n = \cdots = a \cdot k + b \cdot l.$$

Pertanto $d = a \cdot k + b \cdot l,\ \ k, l \in \mathbb{Z}$, con $k, l \in \mathbb{Z}$, cioè che finisce la dimostrazione del teorema. □

Esercizio. Aplicando l'algoritmo di Euclide, si trovi il massimo comune divisore di 2008 e 408; si rappresenti $d = (2008, 408)$ come combinazione lineare di 2008 e 408 a coefficienti in $\mathbb{Z}$.

Soluzione. Si aplica l'algoritmo di Euclide ai numeri 2008 e 408:

$$2008 = 408 \cdot 4 + 376$$

$$408 = 376 \cdot 1 + 32$$

$$376 = 32 \cdot 11 + 24$$

$$32 = 24 \cdot 1 + 8$$

$$24 = 8 \cdot 3.$$

L'ultimo resto non nullo è quindi $d = (2008, 408) = 8$. Per scrivere 8 come combinazione lineare $2008 \cdot k + 408 \cdot l$, con $k, l \in \mathbb{Z}$, separando i resti otteniamo:

$$376 = 2008 - 408 \cdot 4$$

$$32 = 408 - 376$$

$$24 = 376 - 32 \cdot 11$$

$$8 = 32 - 24.$$

Sostituendo successivamente dall'ultima verso la prima uguaglianza si ha:

$$8 = 32 - 24 = 32 - (376 - 32 \cdot 11) = 32 \cdot 12 - 376 = (408 - 376) \cdot 12 - 376 =$$

$$= 408 \cdot 12 - 13 \cdot 376 = 408 \cdot 12 - 13 \cdot (2008 - 408 \cdot 4) = 2008 \cdot (-13) + 408 \cdot 64.$$

Interpretando l'uguaglianza $2008 \cdot (-13) + 408 \cdot 64 = 8$ nel linguaggio delle equazioni, possiamo dire che $x = -13, y = 64$ è una soluzione dell'equazione $2008 \cdot x + 408 \cdot y = 8$.

Problema 1. Un uomo si reca a un fiume con due secchie, una di 7 litri e l' altra di 5 litri. È possibile separare un litro d'acqua in una delle due secchie? Se la risposta è si, dire come.

Soluzione. La risposta è affermativa poiché i due numeri 7 e 5 sono primi tra di loro e quindi esistono x e y, numeri interi tali che $1 = (7, 5) = 7 \cdot x + 5 \cdot y$.

Una possibilità per x e y, oppure una soluzione particolare dell' equazione $7 \cdot x + 5 \cdot y = 1$ (ottenuta mediante l'algoritmo di Euclide), è $(x, y) = (-2, 3)$ perché $1 = 7 \cdot (-2) + 5 \cdot 3$. Per motivi prattici ci serve $x > 0$. Perciò consideriamo la soluzione $x = 3, y = -4$ ottenuta dalle congruenze $-2 \equiv 3 \pmod 5$ e $3 \equiv -4 \pmod 7$,; oppure per tentativi, visto che $1 = 21 - 20 = 7 \cdot 3 + 5 \cdot (-4)$. Questa soluzione ci suggerisce che il secchio di 7 litri sarà riempito tre volte e il secchio di 5 litri sarà svuotato quattro volte. Per comodità indichiamo con S il secchio di 7 litri e con C il secchio di 5 litri.

Detto questo possiamo procedere nel modo seguente:

1) Si riempie la secchia S e poi si versano 5 litri nella secchia C. Si svuota la secchia C. I due litri rimasti nella secchia S si versano nella secchia C.

2) Si riempie la secchia S (per la seconda volta); dalla secchia S si versano 3 litri nella secchia C (dove c'erano già 2 litri) finché si riempie. Poi si svuota la secchia C. I quattro litri rimasti nella secchia S si versano nella secchia C. In questo momento la secchia S è vuota e la secchia C contiene quattro litri.

3) Dalla secchia S, riempita per la terza volta, si versa un litro nella secchia C (finché si riempie di nuovo). Poi si svuota C. Dalla secchia S si versano 5 litri nella secchia C. Così nella secchia S è rimasto solo un litro di acqua. □

II. Equazioni diofantee

In questo paragrafo si studia l'equazione diofantea del primo grado $a \cdot x + b \cdot y = c$ con $a, b, c \in \mathbb{Z}$, in due incognite $x, y \in \mathbb{Z}$. La terminologia risale al nome di Diofante, matematico greco (terzo secolo dopo Cristo) di Alessandria di Egitto. In questo studio il concetto di massimo comune divisore di due numeri interi e le sue propietà sopra presentate (e particolarmente, l'algoritmo di Euclide) saranno i nostri principali strumenti.

Definizione 6. *Sia*

$$a \cdot x + b \cdot y = c, \tag{1}$$

con $a, b, c \in \mathbb{Z}$ *e* $a, b \neq 0$*, un' equazione diofantea di primo grado. Una coppia di numeri interi* (x_0, y_0) *si chiama* soluzione *dell' equazione* (1) *se*

$$a \cdot x_0 + b \cdot y_0 = c,$$

cioè (x_0, y_0) *soddisfa l'equazione* (1).

Esempi. La coppia $(-2, 5)$ è una soluzione dell'equazione $3 \cdot x + 7 \cdot y = 29$, perché vale l'uguaglianza $3 \cdot (-2) + 7 \cdot 5 = 29$; invece $(4, -1)$ non è soluzione perché non regge $3 \cdot 4 + 7 \cdot (-1) = 29$.

Consideriamo i seguenti problemi riguardanti all' equazione (1):

a) Trovare le condizioni necessarie e sufficienti per i coefficienti a, b, c affinché l'equazione (1) ammetta almeno una soluzione.

b) Se l'equazione (1) ammette una soluzione, trovare tutte le soluzioni dell' equazione (1).

c) Indicare un procedimento effettivo di trovare tutte le soluzioni dell' equazione (1).

Consideriamo dapprima lo studio del caso particolare $c = 0$.

Teorema 4 . *L'equazione diofantea omogenea* $a \cdot x + b \cdot y = 0$*, con* $a, b \in \mathbb{Z}^*$*, ammette una infinità di soluzioni e ogni tale soluzione è della forma:*

$$\begin{cases} x = k \cdot \frac{b}{d} \\ y = -k \cdot \frac{a}{d} \\ k \in \mathbb{Z}, \quad d = (a, b) \end{cases} .$$

Dimostrazione. Poniamo $d = (a, b) \in \mathbb{Z}$, e scriviamo $a = d \cdot a_1$, $b = d \cdot b_1$, con $a_1, b_1 \in \mathbb{Z}$. Per la Proposizione 2, (8), a_1 e b_1 sono primi tra di loro, cioè $(a_1, b_1) = 1$. Sostituendo nella equazione iniziale $a \cdot x + b \cdot y = 0$ si ottiene

$$d \cdot a_1 \cdot x + d \cdot b_1 \cdot y = 0 \iff a_1 \cdot x + b_1 \cdot y = 0 \iff a_1 \cdot x = -b_1 \cdot y.$$

Osserviamo che la coppia $(0, 0)$ è, evidentemente una soluzione dell'equazione. Cerchiamo adesso le soluzioni non nulle. Sia dunque $x = u, y = v$ una soluzione non-nulla dell'equazione $a_1 \cdot x + b_1 \cdot y = 0$, cioè $b_1 \cdot v = -a_1 \cdot u$, ciò che implica che b_1 divide il prodotto $a_1 \cdot u$, con b_1 primo con a_1. Risulta $b_1 | u$, cioè $u = b_1 \cdot k$, con $k \in \mathbb{Z}$. Sostituendo si ottiene $b_1 \cdot v = -a_1 \cdot b_1 \cdot k \iff v = -a_1 \cdot k$, cioè $(u, v) = (b_1 \cdot k, -a_1 \cdot k)$.

Viceversa, la coppia $(b_1 \cdot k, -a_1 \cdot k)$ è una soluzione dell' equazione $a \cdot x + b \cdot y = 0$, per ogni $k \in \mathbb{Z}$, poiché $a_1 \cdot (b_1 \cdot k) + b_1 \cdot (-a_1 \cdot k) = 0$.

In conclusione le soluzioni dell'equazione $a \cdot x + b \cdot y = 0$ sono tutte della forma:

$$\begin{cases} x = k \cdot \frac{b}{d} = k \cdot b_1 \\ y = -k \cdot \frac{a}{d} = -k \cdot a_1 \\ k \in \mathbb{Z}, \quad d = (a, b) \end{cases} .$$

□

Passiamo ora allo studio del caso generale $a \cdot x + b \cdot y = c$, con $a, b, c \in \mathbb{Z}^*$.

Teorema 5. *L'equazione* $a \cdot x + b \cdot y = c$*, con* $a, b, c \in \mathbb{Z}^*$ *ammette soluzioni intere se è solo se* $d = (a, b)$ *divide il termine noto c. Se* $d | c$*, l'equazione ammette un'infinità di soluzioni e tutte queste soluzioni sono della forma:*

$$\begin{cases} x = x_0 + k \cdot \frac{b}{d} \\ y = y_0 - k \cdot \frac{a}{d} \\ k \in \mathbb{Z} \end{cases}$$

dove (x_0, y_0) *è una soluzione particolare dell'equazione* (*determinata ad esempio mediante l'algoritmo di Euclide*).

Dimostrazione. Siano $d = (a, b)$ con $a = d \cdot a_1$ e $b = d \cdot b_1$, $(a_1, b_1) = 1$. Applicando l'algoritmo di Euclide ai numeri a_1, b_1, possiamo determinare due numeri interi (u, v) che soddisfano l'equazione, cioè, $a_1 \cdot u + b_1 \cdot v = 1$.

Supponiamo che esiste una soluzione (x_0, y_0) dell'equazione $a \cdot x + b \cdot y = c$, con $a, b, c \in \mathbb{Z}^*$. Quindi $a \cdot x_0 + b \cdot y_0 = c \iff a_1 \cdot d \cdot x_0 + b_1 \cdot d \cdot y_0 = c \iff d \cdot (a_1 \cdot x_0 + b_1 \cdot y_0) = c \implies d|c$.

Viceversa, supponiamo che il massimo comune divizore di a e b divide il termine noto c dell'equazione (1), cioè $(a, b) = d|c$. Allora $c = d \cdot c_1$. Sostituendo nell'equazione $a \cdot x + b \cdot y = c$, si ottiene l'equazione $d \cdot a_1 \cdot x + d \cdot b_1 \cdot y = d \cdot c_1 \iff a_1 \cdot x + b_1 \cdot y = c_1$, equazione delle cui soluzioni ci occuperemo in seguito. Si usa un ragionamento classico: la differenza di due soluzioni dell'equazione generale è soluzione dell'equazione omogenea, già studiata in precedenza.

Siano (x_1, y_1) e (x_0, y_0), con $x_1, y_1, x_0, y_0 \in \mathbb{Z}$, due soluzioni dell'equazione $a_1 \cdot x + b_1 \cdot y = c_1$. Queste soluzioni verificano l'equazione e quindi:

$$\begin{cases} a_1 \cdot x_1 + b_1 \cdot y_1 = c_1 \\ a_1 \cdot x_0 + b_1 \cdot y_0 = c_1, \end{cases}$$

da cui si ottiene $a_1 \cdot (x_1 - x_0) + b_1 \cdot (y_1 - y_0) = 0$. Secondo il caso precedente troviamo

$$\begin{cases} x_1 - x_0 = k \cdot b_1, \\ y_1 - y_0 = -k \cdot a_1, \quad k \in \mathbb{Z}. \end{cases}$$

Denotiamo, invece di (x_1, y_1) con (x, y) una qualunque soluzione. Allora ogni soluzione dell'equazione $a \cdot x + b \cdot y = c$, $a, b, c \in \mathbb{Z}^* \iff a_1 \cdot x + b_1 \cdot y = c_1$ è della forma:

$$\begin{cases} x = x_0 + k \cdot b_1 = x_0 + k \cdot \frac{b}{d} \\ y = y_0 - k \cdot a_1 = y_0 - k \cdot \frac{a}{d} \\ \text{con } k \in \mathbb{Z} \text{ e } (x_0, y_0) \text{ è una soluzione particolare dell'equazione } a_1 \cdot x + b_1 \cdot y = c_1. \end{cases}$$

La soluzione (x_0, y_0) si ottiene moltiplicando l'uguaglianza $a_1 \cdot u + b_1 \cdot v = 1$ (ottenuta eventualmente con l'algoritmo di Euclide) per c_1. Risulta $a_1 \cdot u \cdot c_1 + b_1 \cdot v \cdot c_1 = c_1$ e $x_0 = u \cdot c_1$, $y_0 = v \cdot c_1$.

La dimostrazione del teorema è completa. □

La dimostrazione che segue ci fornisce anche un procedimento effettivo per risolvere le equazioni diofantee $a \cdot x + b \cdot y = c$, con $a, b, c \in \mathbb{Z}^*$:

Passo 1: Si calcola il massimo comune divizore di a e b, cioè $d = (a, b)$.

Passo 2: Si verifica se $d|c$. Se non, l'equazione non ammette soluzioni. Se si, si prosegue con la ricerca delle soluzioni.

Passo 3: Si trova una soluzione particolare (x_0, y_0), dell'equazione $a_1 \cdot x + b_1 \cdot y = c_1$ (eventualmente utilizzando l'algoritmo di Euclide).

Passo 4: Si ricavano le soluzioni dell'equazione $a_1 \cdot x + b_1 \cdot y = 0$, della forma $(k \cdot b_1, -k \cdot a_1)$.

Passo 5: Si ottengono le soluzioni dell'equazione iniziale:

$$\begin{cases} x = x_0 + k \cdot b_1 = x_0 + k \cdot \frac{b}{d} \\ y = y_0 - k \cdot a_1 = y_0 - k \cdot \frac{a}{d} \\ \text{dove k percorre } \mathbb{Z}, \text{ e } (x_0, y_0) \text{ è una soluzione particolare dell'equazione } a_1 \cdot x + b_1 \cdot y = c_1. \end{cases}$$

Gli esercizi che seguono, servono per capire meglio il metodo di risolvere le equazioni diofantee del primo grado.

Esercizi.

1) Si risolvi l'equazione diofantea $4 \cdot x + 6 \cdot y = 10$.

Soluzione. : *Passo* 1: Sia $d = (4, 6) = 2$.

Passo 2: Poiché $2|10$, l'equazione diventa $2 \cdot x + 3 \cdot y = 5$.

Passo 3: La coppia $(x_0, y_0) = (1, 1)$ è una soluzione particolare dell'equazione $2 \cdot x + 3 \cdot y = 5$ $(2 \cdot 1 + 3 \cdot 1 = 5)$.

Passo 4: L'equazione $2 \cdot x + 3 \cdot y = 0$ ammette le soluzioni $x = 3 \cdot k, \;\; y = -2 \cdot k, \;\; k \in \mathbb{Z}$.

Passo 5: In conclusione le soluzioni dell'equazione $4 \cdot x + 6 \cdot y = 10$ sono:

$$\begin{cases} x = 1 + 3 \cdot k \\ y = 1 - 2 \cdot k \\ k \in \mathbb{Z}. \end{cases}$$

Osserviamo che nella ricerca della soluzione particolare non abbiamo utilizzato l'algorimo di Euclide. □

2) Si risolvi l'equazione diofantea $125 \cdot x - 8 \cdot y = 7$.

Soluzione. Passo 1: Calcoliamo $d = (125, 8) = 1$.

Passo 2: L'equazione $125 \cdot x - 8 \cdot y = 7$ ammettte soluzioni poiché $d = 1$ (e quindi $d|7$).

Passo 3: Ricerchiamo una soluzione particolare dell'equazione $125 \cdot x - 8 \cdot y = 7$, mediante l' algoritmo di Euclide:

$$\begin{aligned} 125 &= 8 \cdot 15 + 5, & 5 &= 125 - 8 \cdot 15 \\ 8 &= 5 \cdot 1 + 3, & 3 &= 8 - 5 \cdot 1 \\ 5 &= 3 \cdot 1 + 2, & 2 &= 5 - 3 \cdot 1 \\ 3 &= 2 \cdot 1 + 1, & 1 &= 3 - 2 \cdot 1 \end{aligned}$$

$1 = 3-2 = 3-(5-3) = 3\cdot 2-5 = (8-5)\cdot 2-5 = 8\cdot 2-5\cdot 3 = 8\cdot 2-(125-8\cdot 15)\cdot 3 = 125\cdot(-3)-8\cdot(-47)$.

Quindi $125 \cdot (-3) - 8 \cdot (-47) = 1$. Moltiplicando questa uguaglianza per 7 si ottiene $125 \cdot (-21) - 8 \cdot (-329) = 7$. La coppia $x_0 = -21, \;\; y_0 = -329$ rappresenta una soluzione particolare.

Passo 4: Ne segue che l'equazione $125\cdot x-8\cdot y =$ ammette le soluzioni $x = 8\cdot k, \;\; y = 125\cdot k, \; k \in \mathbb{Z}$.

Passo 5: Le soluzioni dell'equazione $125 \cdot x - 8 \cdot y = 7$ sono:

$$\begin{cases} x = -21 + 8 \cdot k \\ y = -329 - 125 \cdot k \\ k \in \mathbb{Z}. \end{cases}$$

Possiamo considerare la soluzione particolare $(x_0, y_0) = (3, 46)$ $(125\cdot 3-8\cdot 46 = 7)$ ottenuta tramite le congruenze: $-21 \equiv 3 \pmod 8$, $-329 \equiv 46 \pmod{125}$. In questo modo abbiamo :

$$\begin{cases} x = 3 + 8 \cdot k \\ y = 46 - 125 \cdot k \\ k \in \mathbb{Z}. \end{cases}$$

□

3) Si risolvino le seguenti equazioni diofantee:
a) $9 \cdot x + 5 \cdot y = 17 \cdot a$, con $a \in \mathbb{Z}$, fissato.
b) $2 \cdot x + 3 \cdot y = 17 \cdot b$, con $a \in \mathbb{Z}$, fissato.

c) Si dimostri l'uguaglianza di insiemi $\{(x,y)|\ 9\cdot x+5\cdot y = \text{multiplo di } 17\} = \{(x,y)|\ 2\cdot x+3\cdot y = \text{multiplo di } 17\}$.

Soluzione. *I passi* 1 e 2: Entrambe le equazioni ammettono soluzioni poiché $(9,5) = 1$ e $(2,3) = 1$.

Passo 3: Applicando l'algoritmo di Euclide ai numeri 9 e 5 otteniamo $9 \cdot (-1) + 5 \cdot 2 = 1$, e moltiplicando per $17 \cdot a$ otteniamo la seguente soluzione particolare $(x_0, y_0) = (-17 \cdot a, 34 \cdot a)$ per la prime equazione. La coppia $(x_0, y_0) = (-17 \cdot b, 17 \cdot b)$ rappresenta una soluzione particolare per la seconda equazione.

Passo 4: L'equazione omogenea $9 \cdot x + 5 \cdot y = 0$ ammette le soluzioni $x = 5 \cdot k,\ y = -9 \cdot k,\ k \in \mathbb{Z}$; L'equazione omogenea $2 \cdot x + 3 \cdot y = 0$ ammette le soluzioni $x = 3 \cdot l,\ y = -2 \cdot l,\ l \in \mathbb{Z}$.

Passo 5: Le soluzioni dell'equazione $9 \cdot x + 5 \cdot y = 17 \cdot a,\ a \in \mathbb{Z}$, sono

$$\begin{cases} x = -17 \cdot a + 5 \cdot k \\ y = 34 \cdot a - 9 \cdot k \\ k \in \mathbb{Z}. \end{cases}$$

Le soluzioni dell'equazione $2 \cdot x + 3 \cdot y = 17 \cdot b,\ b \in \mathbb{Z}$, sono

$$\begin{cases} x = -17 \cdot b + 3 \cdot l \\ y = 17 \cdot b - 2 \cdot l \\ l \in \mathbb{Z}. \end{cases}$$

Dimostrare l'uguaglianza $\{(x,y)|9\cdot x+5\cdot y = \text{multiplo di } 17\} = \{(x,y)|2\cdot x+3\cdot y = \text{multiplo di } 17\}$ del punto *c)* significa dimostrare che le equazioni $9\cdot x+5\cdot y \equiv 0 \pmod{17}$ e $2\cdot x+3\cdot y \equiv 0 \pmod{17}$ ammettono le stesse soluzioni.

Sostituendo le soluzioni della prima equazione (sopra ottenute) nella seconda equazione, si ha:

$$2 \cdot (-17 \cdot a + 5 \cdot k) + 3 \cdot (34 \cdot a - 9 \cdot k) = -17 \cdot k \equiv 0 \pmod{17},$$

(cioè le soluzioni della prima equazione soddisfano la seconda equazione). Viceversa, sostituendo nella prima equazione le soluzioni della seconda equazione, otteniamo

$$9 \cdot (-17 \cdot b + 3 \cdot l) + 5 \cdot (17 \cdot b - 2 \cdot l) = 17 \cdot l \equiv 0 \pmod{17},$$

(cioè le soluzioni della seconda equazione soddisfano la prima equazione). In questo modo abbiamo dimostrato, per doppia inclusione, l'uguaglianza dei due insiemi.

Abbiamo visto che le due equazioni sono equivalenti nel senso che hanno le stesse soluzioni; però avremmo potuto dimostrare che le due equazioni sono equivalenti (senza trovare le loro soluzioni) osservando che molteplichiamo per 4 la congruenza $9 \cdot x + 5 \cdot y \equiv 0 \pmod{17}$, si ritrova la seconda equazione $2 \cdot x + 3 \cdot y \equiv 0 \pmod{17}$, poiché $36 \equiv 2 \pmod{17}$ e $20 \equiv 3 \pmod{17}$.

Il punto c) può essere anche riformulato nel modo seguente: dimostrare che la congruenza $9 \cdot x + 5 \cdot y \equiv 0 \pmod{17}$ è equivalente alla congruenza $2 \cdot x + 3 \cdot y \equiv 0 \pmod{17}$. In questo modo la risoluzione del problema diventa più semplice. Infatti, poiché $(4, 17) = 1$, ne segue che 4 è invertibile in R_{17} e quindi

$$9 \cdot x + 5 \cdot y \equiv 0 \pmod{17} \iff 36 \cdot x + 20 \cdot y \equiv 0 \pmod{17} \iff 2 \cdot x + 3 \cdot y \equiv 0 \pmod{17}. \ \square$$

4) Si determini il minimo numero naturale n, tale che l'equazione $1001\cdot x+770\cdot y = 1000000+n$ ammetta soluzioni. Dimostrare che questa equazione, con n minimo sopra determinato, ammette 100 soluzioni nel primo quadrante (oppure $x > 0,\ y > 0$).

Soluzione. L'equazione $1001 \cdot x + 770 \cdot y = 1000000 + n$ può essere riscritta sotto la forma $77\cdot 13\cdot x+77\cdot 10\cdot y = 10^6+n \iff 77\cdot(13\cdot x+10\cdot y) = 10^6+n$. Quest' ultima equazione ammette

soluzioni se e solo se $77|(10^6+n)$. Abbiamo $10^6 = 77 \cdot 12987 + 1$ e $77 \cdot 12988 = 1000076$. Perciò, il valore minimo di n è 76. In questo caso l'equazione diventa $1001 \cdot x + 770 \cdot y = 1000000 + 76 \iff 13 \cdot x + 10 \cdot y = 12988$.

Passi 1 e 2: Calcoliamo $d = (13, 10) = 1$ (che divide 12988), e quindi l'equazione ammette soluzioni.

Passo 3: Dall' uguaglianza $13 \cdot (-3) + 10 \cdot 4 = 1$, molteplicata per 12988, si ottiene la seguente soluzione particolare $(x_0, y_0) = (-38964, 51952)$ dell' equazione $13 \cdot x + 10 \cdot y = 12988$.

Passo 4: L'equazione omogenea $13 \cdot x + 10 \cdot y = 0$ ammette le soluzioni $x = 10 \cdot k, \quad y = -13 \cdot k, \quad k \in \mathbb{Z}$.

Passo 5: Allora le soluzioni dell'equazione non omogenea sono:

$$\begin{cases} x = -38964 + 10 \cdot k \\ y = 51952 - 13 \cdot k \\ k \in \mathbb{Z} \end{cases} .$$

Dalle condizioni $x > 0, y > 0$ si ottiene il sistema

$$\begin{cases} -38964 + 10 \cdot k > 0 \\ 51952 - 13 \cdot k > 0 \end{cases} \iff \begin{array}{l} 10 \cdot k > 38964 \\ 13 \cdot k < 51952 \end{array} \iff 3897 \leq k \leq 3996$$

Poiché l'intervallo $[3897, 3996]$ contiene esattamente 100 numeri interi, concludiamo che l'equazione $13 \cdot x + 10 \cdot y = 12988$ ammette precisamente 100 soluzioni nel primo quadrante. □

5) Si determinino tutte le funzioni $f : \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{N}^*$ che soddisfano le seguenti condizioni:

$$\begin{cases} (i)\ f(x, x) = x \\ (ii)\ f(x, y) = f(y, x) \\ (iii)\ f(x, y) = f(x, x + y). \end{cases}$$

Soluzione. Lo studio di alcuni casi particolari ci suggerisce che $f(x, y)$ è il massimo comune divisore di x e y. Dimostriamo per induzione secondo $n = x+y$ che ogni funzione che soddisfa le tre proprietà dell' ipotesi del problema è "il massimo comune divisore". Denotiamo con $g(x, y) = (x, y)$ il massimo comune divisore di x e y. Allora valgono le seguenti uguaglianze: $f(1, 1) = 1 = g(1, 1)$, $f(1, 1) = f(1, 1 + 1) = f(1, 2) \Longrightarrow f(1, 2) = g(1, 2)$. Assumiamo l'asserzione vera per ogni $x, y \in \mathbb{N}^*$, tali che $2 < x + y \leq k$, con k fissato. Bisogna dimostrare che $f(x, y) = g(x, y)$, per $x + y = k + 1$. L' ipotesi di simmetria $f(x, y) = f(y, x)$ ci permette assumere (senza restringere la generalità) che $x < y$. Da (iii) si ottiene $f(x, y) = f(x, x + (y - x)) = f(x, y - x)$. Siccome $x + (y - x) = y < y + x = k + 1 \implies x + (y - x) \leq k$ possiamo applicare l'ipotesi di induzione e troviamo $f(x, y - x) = g(x, y - x)$.

Rimane da dimostrare che $g(x, y - x) = g(x, y)$. Siano $d = (x, y)$ e $d_1 = (x, y - x)$. Da $d|x$, $d|y$ risulta $d|x$ e $d|(y - x)$, e quindi $d|(x, y - x)$, cioè $d|d_1$. Viceversa, da $d_1|x$ e $d_1|(y - x)$ risulta $d_1|(x + y - x)$, cioè $d_1|x$ e $d_1|y$ oppure ancora $d_1|d$. Abbiamo ottenuto $d|d_1$ e $d_1|d$ e quindi $d = d_1$.

In conclusione abbiamo dimostrato che $f(x, y) = f(x, y - x) = g(x, y - x) = g(x, y)$, con $x + y = k + 1$. Per il teorema di induzione (forma forte), risulta $f(x, y)$ coincide con il massimo comune divisore di x e y. □

Interpretazione geometrica delle equazioni diofantee. L'equazione $a \cdot x + b \cdot y = c$ (con $a \neq 0$ o $b \neq 0$) definisce una retta nel piano cartesiano. La risoluzione in numeri interi, dell'equazione $a \cdot x + b \cdot y = c$ equivale a trovare i punti di coordinate numeri interi, che appartengono alla retta di equazione $a \cdot x + b \cdot y = c$.

I punti del piano cartesiano di coordinate numeri interi si chiamano punti laticeali. Per esempio, i punti di coordinate $(2, -5)$, $(0, 0)$ e $(1, 7)$ sono punti laticeali, mentre i punti di coordinate $(\frac{2}{3}, -1)$ e $(7, \sqrt{2})$ non sono punti laticeali.

Sia (x_0, y_0) un punto laticeale fissato, apartenente alla retta di equazione $a \cdot x + b \cdot y = c$ (supponiamo che esista). Abbiamo $a \cdot x_0 + b \cdot y_0 = c$. Ogni altro punto laticeale (x_1, y_1) appartiene alla retta, se e solo se, la pendenza (o il coefficiente angolare) $\frac{y_1 - y_0}{x_1 - x_0}$ della retta è uguale a $\frac{-a}{b}$, ossia, alla frazione irriducibile $\frac{\frac{a}{d}}{\frac{b}{d}}$, dove $d = (a, b)$. In alte parole,

$$\frac{y_1 - y_0}{x_1 - x_0} = \frac{\frac{a}{d}}{\frac{b}{d}}.$$

Ogni frazione razionale si ottiene da una frazione irriducibile amplificandola per un numero intero. Allora l'uguaglianza precedente diventa

$$\begin{cases} x_1 - x_0 = k \cdot \frac{b}{d} \\ y_1 - y_0 = k \cdot \frac{a}{d} \end{cases} .$$

In questo modo si ottengono le soluzioni interi dell'equazioni $a \cdot x + b \cdot y = c,\ a, b, c \in \mathbb{Z}$, a meno che l'equazione ammetta una soluzione intera. Per esempio, la retta di equazione $2 \cdot x + 4 \cdot y = 3$ non contiene nessun punto laticeale. □

III. Congruenze

In questo paragrafo presentiamo la "*congruenza modulo n*" e le sue applicazioni alla risoluzione delle equazioni in congruenza modulo n. La parola congruenza è già nota dalla geometria: due figure piane si chiamano congruenti se sovrapponendole (mediante le traslazioni, rotazioni o simmetrie) coincidono, cioè due figure sono congruenti se sono "uguali a meno di uno spostamento". Da qui risulta che due segmenti sono congruenti se hanno la stessa lunghezza, due angoli sono congruenti se hanno la stessa misura.

Definizione 7. *Sia $n \geq 2$ un numero naturale fissato. Due numeri interi a e b si chiamano* congruenti modulo n *(e si scrive $a \equiv b \pmod{n}$), se e solo se a e b hanno lo stesso resto rispetto alla divisione con n.*

Per esempio: $32 \equiv 102 \pmod{5}$ poiché $32 = 5 \cdot 6 + 2$ e $102 = 5 \cdot 20 + 2$

$47 \equiv 190 \pmod{11}$ poiché $47 = 11 \cdot 4 + 3$ e $190 = 11 \cdot 17 + 3$.

$-73 \equiv (-1) \equiv 107 \pmod{12}$ poiché $-73 = 12 \cdot (-8) + 11$, $-1 = 12 \cdot (-1) + 11$, $107 = 12 \cdot 8 + 11$.

In generale si ha $n \equiv 0 \pmod{n}$ e $-1 \equiv (n-1) \pmod{n}$, per ogni numero naturale $n \geq 2$. Osservando che due numeri interi hanno lo stesso resto nella divisione con $n \in \mathbb{N}^*$ se e solo se la loro differenza si divide per n, possiamo riformulare la definizione precedente come segue:

$$a \equiv b \pmod{n} \iff a - b = k \cdot n, \text{ con } k \in \mathbb{Z} \iff a - b \text{ è multiplo di } n \iff (a - b) | n.$$

Siccome in geometria si usa l'espressione "segmenti uguali a meno una trasformazione" per i segmenti congruenti, si può dire altrettanto per due numeri congruenti modulo n, cioè "numeri uguali a meno un multiplo di n" (più precisamente, uno si ottiene dall'altro sommandogli un multiplo di n: $a = b + k \cdot n, k \in \mathbb{Z}$).

Proposizione 3. *La relazione di "congruenza modulo n" è una relazione di equivalenza (cioè riflessiva, simmetrica e transitiva), compatibile con l'addizione e con la moltiplicazione dei numeri interi:*

1) $a \equiv a \pmod{n}$ *per ogni* $a \in \mathbb{Z}$ (*riflessività*),

2) *Se* $a \equiv b \pmod{n}$ *allora anche* $b \equiv a \pmod{n}$ (*simmetria*),

3) *Se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$ *allora* $a \equiv c \pmod{n}$ (*transitività*),

4) *Se* $a \equiv b \pmod{n}$ *allora per ogni numero* $c \in \mathbb{Z}$ *valgono le relazioni:*

$$a + c \equiv b + c \pmod{n} \text{ (\textit{compatibilità con l'addizione}) } e$$

$$a \cdot c \equiv b \cdot c \pmod{n} \text{ (\textit{compatibilità con la moltiplicazione}) .}$$

Altre proprietà della congruenza modulo n*:*

5) *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$ *allora*

$$a + c \equiv b + d \pmod{n} \quad e \quad a \cdot c \equiv b \cdot d \pmod{n}$$

(*Due congruenze si possono sommare o molteplicare a membro a membro*).

6) *Se* $a \equiv b \pmod{n}$ *e* $m \in \mathbb{N}$ *allora* $a^m \equiv b^m \pmod{n}$*. L'affermazione reciproca è in generale falsa.*

7) *Da* $x \equiv y \pmod{n}$ *non risulta in generale* $a^x \equiv a^y \pmod{n}$*.*

Dimostrazione. Per la definizione della congruenza modulo n si ha

$$a \equiv b \pmod{n} \Longleftrightarrow a - b = k \cdot n, k \in \mathbb{Z}, \Longleftrightarrow n|(a - b).$$

1) $a \equiv a \pmod{n} \Longleftrightarrow a - a = 0 = 0 \cdot n$, ciò che è evidentemente vero.

2) $a \equiv b \pmod{n} \Longleftrightarrow a - b = k \cdot n,\ k \in \mathbb{Z} \Longleftrightarrow b - a = (-k) \cdot n \Longleftrightarrow b \equiv a \pmod{n}$.

3) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ allora $a - b = k \cdot n$ e $b - c = l \cdot n$ cu $k, l \in \mathbb{Z}$. Sommando a membro a membro le due uguaglianze si ottiene $a - c = (k + l) \cdot n$ e quindi $a \equiv c \pmod{n}$.

4) Siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$, oppure $a - b = k \cdot n,\ k \in \mathbb{Z}$. Possiamo scrivere $(a + c) - (b + c) = k \cdot n$ e $a \cdot c - b \cdot c = (k \cdot c) \cdot n$; ne risulta $a + c \equiv b + c \pmod{n}$ e $a \cdot c \equiv b \cdot c \pmod{n}$.

5) Siano $a, b, c, d \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Risulta $a - b = k \cdot n$ e $c - d = l \cdot n$ con $k, l \in \mathbb{Z}$. Sommando le ultime due uguaglianze a membro a membro otteniamo $(a+c)-(b+d) = (k+l)\cdot n$, e quindi si trova $a+c \equiv b+d \pmod{n}$. Moltiplicando le relazioni $a - b = k \cdot n$ con c e $c - d = l \cdot n$ con b e sommando le due uguaglianze ottenute, troviamo $a \cdot c - b \cdot d = (kc + lb) \cdot n$; ne segue $a \cdot c \equiv b \cdot d \pmod{n}$.

6) Siano $a, b \in \mathbb{Z}$ e $k \in \mathbb{N}^*$ tali che $a \equiv b \pmod{n}$. Dalla proprietà 5) risulta $a^2 \equiv b^2 \pmod{n}$. Supponiamo la tesi vera per un $l \geq 2$ fissato, cioè $a^l \equiv b^l \pmod{n}$. Siccome sappiamo ache che $a \equiv b \pmod{n}$, per la proprietà 2), risulta $a^{l+1} \equiv b^{l+1} \pmod{n}$. Per il teorema dell'induzione matematica si conclude $a^k \equiv b^k \pmod{n}$ per ogni $k \in \mathbb{N}^*$. Per dimostrare che l' affermazione reciproca è in generale falsa, basta considerare l'esempio seguente: $3^4 \equiv 7^4 \pmod{10}$ e pure, $3 \not\equiv 7 \pmod{10}$.

7) Basta considerare l'esempio seguente: benché $2 \equiv 7 \pmod{5}$ si ha $2^2 \not\equiv 2^7 \pmod{5}$ o $3^2 \not\equiv 3^7 \pmod{5}$. Per evitare i calcoli scriviamo $3^7 = 3^4 \cdot 3^3 \equiv 1 \cdot 27 \pmod{5} \equiv 2 \pmod{5}$. □

Commento. La quinta proprietà afferma che due congruenze modulo n si possono sommare e moltiplicare a membro a membro (come le uguaglianze); inoltre per semplificare i calcoli, si usano i numeri ridotti modulo n.

Esempi.

1) $52 \equiv 6 \pmod{23}$,

2) $-52 = -23 \cdot 2 - 6 \equiv -6 \pmod{23} \equiv 23 - 6 \pmod{23} \equiv 17 \pmod{23}$,

3) $-65 \equiv 16 \pmod{81}$,

4) $43 + 68 + 25 - 57 \cdot 2698 = [(7 \cdot 6 + 1) + (7 \cdot 9 + 5) + (7 \cdot 3 + 4) - (7 \cdot 8 + 1)(7 \cdot 385 + 3)] \equiv (1 + 5 + 4 - 1 \cdot 3) \pmod 7 \equiv 7 \pmod{7} \equiv 0 \pmod{7}$.

Osservazione. L'insieme dei resti modulo n è l'insieme dei resti nella divisione con n, cioè l'insieme $R_n = \{k \mid 0 \leq k < n\} = \{0, 1, 2, ..., n-1\}$. Sottolineamo che R_n contiene esattamente n elementi. Sull'insieme, R_n, dei resti modulo n, si definiscono le operazioni di addizione, sottrazione e moltiplicazione modulo n, nel modo seguente:

- $a + b =$ il resto della divisione di $a + b$ per n,
- $a - b =$ il resto della divisione di $a - b$ per n,
- $a \cdot b =$ il resto della divisione di $a \cdot b$ per n.

Esempi. Sia $n = 12$.

1) $7 + 11 \cdot 3 = 40 \equiv 4 \pmod{12}$,

2) $7 \cdot 5 \equiv 11 \pmod{12}$,

3) $5 \cdot 5 \equiv 1 \pmod{12}$,

4) $6 \cdot 4 \equiv 0 \pmod{12} \equiv 6 \cdot 8 \pmod{12}$ e $4 \not\equiv 8 \pmod{12}$.

L'ultimo esempio ci avvertisce che in una congruenza non si può semplificare sempre. Più avanti dimostreremo che se a e n sono tali che $(a, n) = 1$, allora vale la seguente implicazione

$$a \cdot b \equiv a \cdot c \pmod{n} \implies a \equiv b \pmod{n}.$$

Esercizi.

1) Si trovi il resto della divisione di 5^{7^n} per 31, dove $n \in \mathbb{N}$.

Soluzione. La potenza di 5 più vicina a un multiplo di 31 è $5^3 = 125 = 31 \cdot 4 + 1 \equiv 1 \pmod{31}$. Perciò $7^n \equiv (3 \cdot 2 + 1)^n \pmod 3 \equiv 1^n \pmod 3 \equiv 1 \pmod 3$, e quindi $7^n = 3 \cdot k + 1, k \in \mathbb{N}^*$. Risulta $5^{7^n} \equiv 5^{3 \cdot k+1} \pmod{31} \equiv (5^3)^k \cdot 5 \pmod{31} \equiv 125^k \cdot 5 \equiv 1^k \cdot 5 \pmod{31} \equiv 5 \pmod{31}$. Di conseguenza, il resto della divisione del numero 5^{7^n} per 31 è uguale a 5, per ogni $n \in \mathbb{N}$. □

2) Si dimostri che il resto della divisione di $10^n - 1$ per 37 è un quadratto perfetto, per ogni numero naturale n.

Soluzione. Da $10^3 = 37 \cdot 27 + 1$ risulta $10^3 \equiv 1 \pmod{37}$. Ogni numero naturale n può essere scritto sotto la forma $n = 3 \cdot k + r$ dove $k \in \mathbb{N}$ e $r \in \{0, 1, 2\}$. Ne segue $10^n - 1 \equiv 10^{3 \cdot k+r} - 1 \pmod{37} \equiv (10^3)^k \cdot 10^r - 1 \pmod{37} \equiv 1^k \cdot 10^r - 1 \pmod{37} \equiv 10^r - 1 \pmod{37}$.

Per $r = 0$ abbiamo $10^0 - 1 \equiv 0 \equiv 0^2 \pmod{37}$,
per $r = 1$ abbiamo $10^1 - 1 \equiv 9 \equiv 3^2 \pmod{37}$
e per $r = 2$ abbiamo $10^2 - 1 \equiv 99 \equiv 5^2 \pmod{37}$, e quidi la tesi. □

3) Si dimostri che per ogni $n \in \mathbb{N}^*$, $2^{2 \cdot n+1} + 1$ è un multiplo di 3.

Soluzione. Basta dimostrare che $2^{2 \cdot n+1} + 1 \equiv 0 \pmod 3$. Abbiamo: $2^{2 \cdot n+1} + 1 \equiv (2^2)^n \cdot 2 + 1 \pmod 3 \equiv 4^n \cdot 2 + 1 \pmod 3 \equiv 1^n \cdot 2 + 1 \pmod 3 \equiv 0 \pmod 3$. □

4) Si dimostri che per ogni numero naturale n, il numero $6^{2 \cdot n+1} + 1$ è divisibile per 7.

Soluzione. $6^{2 \cdot n+1} + 1$ è divisibile per 7, se e solo se $6^{2 \cdot n+1} + 1 \equiv 0 \pmod 7$. Abbiamo: $6^{2 \cdot n+1} + 1 \equiv (-1)^{2 \cdot n+1} + 1 \pmod 7 \equiv -1 + 1 \pmod 7 \equiv 0 \pmod 7$. □

5) Si dimostri che per ogni $n \in \mathbb{N}$, $7^{2\cdot n} - 1$ è divisibile per 48.

Soluzione. $7^{2\cdot n} - 1 = (7^2)^n - 1 = 49^n - 1 \equiv 1^n - 1 \pmod{48} \equiv 0 \pmod{48}$, e quindi $7^{2\cdot n} - 1$ è divisibile per 48. □

6) Si dimostri che per ogni numero primo p e per ogni $k \in \mathbb{N}$, $1 \leq k \leq p-1$, $C_p^k \equiv 0 \pmod{p}$.

Soluzione. Per ogni $k \in \mathbb{N}$, $1 \leq k \leq (p-1)$ e p primo risulta che k è primo con p. Dalla relazione $k \cdot C_p^k = p \cdot C_{p-1}^{k-1}$ si ottiene che $p | k \cdot C_p^k$. Poiché p primo e $1 \leq k \leq p$ implica $(k, p) = 1$, risulta $p | C_p^k$. Questo significa che $C_p^k \equiv 0 \pmod{p}$. □

I resti modulo n, cioè $0, 1, 2, 3, \ldots, n-1$, giocano per i numeri interi lo stesso ruolo come le frazioni irriducibili per le frazioni razionali: siccome ogni frazione razionale puo essere semplificata in modo che il numeratore e il denominatore della frazione ridotta siano primi tra di loro, vale altrettanto che ogni numero intero può essere ridotto modulo n in modo tale che diventi congruo a uno dei resti $0, 1, 2, 3, \ldots, n-1$.

È ben noto che nell'insieme dei numeri interi $\mathbb{Z}$, dalle condizioni $a \cdot c = b \cdot c$ e $c \neq 0$ segue $a = b$. In altre parole, se un prodotto di numeri interi è uguale a zero allora almeno un fattore è uguale a zero, cioè $[a \cdot b = 0] \Longleftrightarrow [a = 0 \text{ oppure } b = 0]$. Più esplicitamente: se $c \neq 0$, nella relazione $a \cdot c = b \cdot c$ si può semplificare per c. Questa proprietà non è più valida in generale per le congruenze come fa vedere l'esempio seguente: $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$ benché $2 \not\equiv 4 \pmod{6}$.

Nel seguito daremo una condizione necessaria e sufficiente affinchè si possa semplificare in una congruenza, cioè daremo delle condizioni per c affinchè dalla relazione $a \cdot c \equiv b \cdot c \pmod{n}$ risulti $a \equiv b \pmod{n}$.

Osserviamo innanzitutto che nel insieme dei numeri reali, dall'uguaglianza $a \cdot c = b$ con $c \neq 0$, moltiplicandola per $\frac{1}{c}$ si ricava $a = \frac{b}{c}$. Il numero $\frac{1}{c}$ si chiama l'inverso di c rispetto alla moltiplicazione dei numeri reali.

Così siamo condotti alla seguente definizione:

Definizione 8. *Un elemento $a \in R_n$ si dice invertibile (rispetto alla moltiplicazione di R_n) se esiste un elemento $b \in R_n$ tale che $a \cdot b \equiv 1 \pmod{n}$.*

Per esempio $3 \cdot 7 \equiv 1 \pmod{10}$. Viene fuori la seguente domanda: esiste un altro resto b in R_{10} diverso da 7 tale che $3 \cdot b \equiv 1 \pmod{10}$? La risposta (che in effetti riguarda l'unicità) è data dalla seguente:

Osservazione. *Se un elemento $a \in R_n$ è invertibile (rispetto alla moltiplicazione), allora ammette un unico inverso.*

Infatti, supponiamo che esistano $b, c \in R_n$ tali che $a \cdot b \equiv 1 \pmod{n}$ e $a \cdot c \equiv 1 \pmod{n}$. Moltiplicando la prima equivalenza per c e la seconda per b, abbiamo

$$a \cdot b \cdot c \equiv c \pmod{n} \quad \text{e} \quad a \cdot c \cdot b \equiv b \pmod{n}.$$

Da qui si ricava $c \equiv b \pmod{n}$. Siccome $b, c \in R_n$ risulta $b = c$. □

Diamo ora una condizione necessaria e sufficiente affinchè un resto $a \in R_n$ sia invertibile:

Proposizione 4. *Sia $a \in R_n$. Allora a è invertibile se e solo se a è primo con n (in altre parole, se e solo se il massimo comune divisore di a e n è uguale a 1).*

Dimostrazione. Sia $a \in R_n$ invertibile. Allora esiste $b \in R_n$ tale che $a \cdot b \equiv 1 \pmod{n}$, cioè $a \cdot b - 1 = k \cdot n$, con $k \in \mathbb{Z}$, o ancora, $a \cdot b - k \cdot n = 1$. Sia d un divizore comune di a e n. Dalle condizioni $d|a$ e $d|n$ risulta $d|(a \cdot b - k \cdot n)$, cioè $d|1$ e quindi $d = 1$. Prima implicazione è dimostrata.

Dimostriamo ora l'implicazione opposta. Supponiamo che a e n sono primi tra di loro, cioè $d = (a, n) = 1$. Applicando l'algoritmo di Euclide ai numeri a e n si trovano $b, c \in \mathbb{Z}$ tali che

$$a \cdot b + n \cdot c = 1 \Longleftrightarrow a \cdot b = 1 - n \cdot k \equiv 1 \pmod{n},$$

e quindi, a è invertibile. □

Corollario. *Se a e n sono due numeri naturali tali che $(a,b)=1$ e se $x,y\in\mathbb{Z}$ sono due interi tali che $a\cdot x\equiv a\cdot y \pmod{n}$, allora $x\equiv y \pmod{n}$.*

Dimostrazione. Se a è primo con n allora a è invertibile; sia $b\in R_n$ l'inverso di a. Moltiplicando la congruenza $a\cdot x\equiv a\cdot y \pmod{n}$ per b otteniamo $b\cdot a\cdot x\equiv b\cdot a\cdot y \pmod{n}$, ciò che implica $x\equiv y \pmod{n}$. □

Esempi.

1) Gli elementi invertibili di R_9 sono $1,2,4,5,7,8$. Inoltre:
   l'inverso di 1 è 1 poiché $1\cdot 1\equiv 1 \pmod{9}$,
   l'inverso di 2 è 5 poiché $2\cdot 5\equiv 1 \pmod{9}$,
   l'inverso di 4 è 7 poiché $4\cdot 7\equiv 1 \pmod{9}$,
   l'inverso di 8 è 8 poiché $8\cdot 8\equiv \pmod{9}$.

2) Gli elementi invertibili di R_{12} sono $1,5,7,11$ e inoltre:
   l'inverso di 1 è 1 poiché $1\cdot 1\equiv 1 \pmod{12}$,
   l'inverso di 5 è 5 poiché $5\cdot 5\equiv 1 \pmod{12}$,
   l'inverso di 7 è 7 poiché $7\cdot 7\equiv 1 \pmod{12}$,
   l'inverso di 11 è 11 poiché $11\cdot 11\equiv 1 \pmod{12}$.

Corollario. Sia $p\in\mathbb{N}$ un numero primo. Allora l'insieme degli elementi invertibili di R_p è $R_p^*=\{1,2,3,\dots,(p-1)\}$.

Dimostrazione. Tutto segue dal fatto che ogni k, con $1\le k\le p-1$, è primo con p. □

Equazioni in congruenza modulo n.

Andiamo a studiare le equazioni del tipo $a\cdot x\equiv b \pmod{n}$, con $a,b\in\mathbb{Z}$ e $n\in\mathbb{N}^*$.

Definizione. *Si dice soluzione dell'equazione $a\cdot x\equiv b \pmod{n}$ un elemento $c\in\mathbb{Z}$ che soddisfa la congruenza $a\cdot c\equiv b \pmod{n}$. Due soluzioni $c_1,c_2\in\mathbb{Z}$ sono non equivalenti se non sono congruenti modulo n, cioè $c_1\not\equiv c_2 \pmod{n}$. Osserviamo che se $u\neq v\in R_n$, allora u non è congruo a v modulo n. Osserviamo che nell' equazione $a\cdot x\equiv b \pmod{n}$ possiamo sempre suppore che a e b appartengono a R_n.*

Per esempio, i numeri $3,7$ e 43 sono soluzioni dell'equazione $2\cdot x\equiv 6 \pmod{8}$ poiché $2\cdot 3\equiv 6 \pmod{8}$, $2\cdot 7\equiv 6 \pmod{8}$, $2\cdot 43\equiv 6 \pmod{8}$; inoltre, $3\equiv 43 \pmod{8}$ e $3\not\equiv 7 \pmod{8}$.

Cominciamo con lo studio di un caso particolare: l'equazione $4\cdot x\equiv 3 \pmod{9}$ ammette una sola soluzione in R_9, come è facile vedere (poiché R_9 contiene solo nove elementi). Equivalentemente, moltiplicando per l'inverso di 4 (che è 7) troviamo $7\cdot 4\cdot x\equiv 7\cdot 3 \pmod{9} \iff x\equiv 3 \pmod{9}$.

Teorema 6. *L'equazione $a\cdot x\equiv b \pmod{n}$ ammette soluzioni se e solo se $d=(a,n)$ divide b. In tal caso l'equazione ammette esatamente d soluzioni non equivalenti, che sono della forma*

$$x_0,\ \ x_0+\frac{n}{d},\ \ x_0+2\cdot\frac{n}{d},\ \ x_0+3\cdot\frac{n}{d},\dots,x_0+(d-1)\cdot\frac{n}{d},$$

con x_0 una soluzione particolare dell' equazione $a\cdot x-n\cdot y=b$.

Dimostrazione. L'equazione $a\cdot x\equiv b \pmod{n}$ è equivalente all'equazione diofantea $a\cdot x-n\cdot y=b$, che (come già sappiamo) ammette soluzioni se e solo se $d=(a,n)$ divide b.

Siano $a=d\cdot a_1$, $n=d\cdot n_1$ e $b=d\cdot b_1$. Per la Proposizione 2, (8), sappiamo che a_1 e n_1 sono primi tra di loro, cioè $(a_1,n_1)=1$. Sostituendo, si ottiene l'equazione

$$d\cdot a_1\cdot x-d\cdot n_1=d\cdot b_1 \iff a_1\cdot x-n_1\cdot y=b_1.$$

Sia ora (x_0, y_0) una soluzione particolare dell' equazione $a_1 \cdot x - n_1 \cdot y = b_1$, ricavata eventualmente applicando l'algoritmo di Euclide ai numeri a_1 e n_1. Le soluzioni dell'equazione $a_1 \cdot x - n_1 \cdot y = b_1$ esistono e sono della forma $x = x_0 + n_1 \cdot k, \quad y = y_0 + a_1 \cdot k$, con k percorrendo l'insieme dei numeri interi $\mathbb{Z}$.

Affermazione: ogni due numeri distinti appartenenti a $\{x_0, x_0+n_1, x_0+2\cdot n_1, \ldots, x_0+(d-1)\cdot n_1\}$ non sono congruenti modulo n.

Infatti, supponiamo che $x_0 + n_1 \cdot k \equiv x_0 + n_1 \cdot l \pmod{n}$, cu $0 \leq l < k \leq d-1$. Risulta $n_1 \cdot (k-l) = n \cdot m$, $m \in \mathbb{N}^*$, o ancora, $n_1 \cdot (k-l) = d \cdot n_1 \cdot m \iff k - l = d \cdot m$. Otteniamo $d \cdot m = k - l < d \leq d \cdot m$, cioè $d \cdot m < d \cdot m$, un assurdo.

Sia ora $k \in \mathbb{Z}$. Dividendo k per d col resto, si ha $k = d \cdot q + r$, $q \in \mathbb{Z}$, $0 \leq r < d$. Ne segue che $k \equiv r \pmod{d}$, e quindi $x_0 + k \cdot n_1 \equiv x_0 + r \cdot n_1 \pmod{n}$.

In conclusione l'equazione $a \cdot x \equiv b \pmod{n}$, con $d = (a, n) | b$, ammette d soluzioni ed esse sono della forma

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad x_0 + 3 \cdot \frac{n}{d}, \quad \ldots, x_0 + (d-1) \cdot \frac{n}{d}. \qquad \square$$

Osservazione importante. Se $(a, n) = 1$, esiste $k \in \{1, 2, \ldots, n-1\}$ tale che $a \cdot k \equiv 1 \pmod{n}$. Infatti, $(a, n) = 1 \iff \exists\, u, v \in \mathbb{Z}$ tali che $a \cdot u + n \cdot v = 1$. Sia $k \in \{1, 2, \ldots, n-1\}$, $k \equiv u \pmod{n}$. Allora $a \cdot k \equiv 1 \pmod{n}$, e quindi k è l'inverso di a in R_n.

Conseguenza. Se a è primo con n, l'equazione $a \cdot x \equiv b \pmod{n}$ ammette una soluzione unica $x \equiv k \cdot b \pmod{n}$, dove k è l'inverso di a in R_n.

Applicazioni. Si risolvino le seguenti equazioni:

$$2 \cdot x \equiv 3 \pmod{5}, \quad 4 \cdot x \equiv 4 \pmod{8}, \quad 4 \cdot x \equiv 6 \pmod{8}, \quad 357 \cdot x \equiv 12 \pmod{510}.$$

Soluzione. L'equazione $2 \cdot x \equiv 3 \pmod{5}$ ammette una sola soluzione in R_5 perché 5 è numero primo e quindi 2 è invertibile. In questo caso, il modo più veloce di trovare l'inverso di 2 in R_5, è di costruire la tavola di moltiplicazione per 2 in R_5: $2 \cdot 1 \equiv 2 \pmod{5}$, $2 \cdot 2 \equiv 4 \pmod{5}$, $2 \cdot 3 \equiv 1 \pmod{5}$, $2 \cdot 4 \equiv 3 \pmod{5}$; da qui si ricava la soluzione $x \equiv 4 \pmod{5}$.

L'equazione $4 \cdot x \equiv 4 \pmod{8}$ ammette 4 soluzioni perché $d = (4, 8) = 4$ divide 4. Anche in questo caso, costruendo la tavola di moltiplicazione per 4 in R_8 si trovano le soluzioni:

$$4 \cdot 1 \equiv 4 \pmod{8}, \quad 4 \cdot 2 \equiv 0 \pmod{8}, \quad 4 \cdot 3 \equiv 4 \pmod{8},$$

$$4 \cdot 4 \equiv 0 \pmod{8}, \quad 4 \cdot 5 \equiv 4 \pmod{8}, \quad 4 \cdot 6 \equiv 0 \pmod{8}, \quad 4 \cdot 7 \equiv 4 \pmod{8}.$$

Perciò, le soluzioni dell'equazione $4 \cdot x \equiv 4 \pmod{8}$ sono $x \equiv 1 \pmod{8}$, $x \equiv 3 \pmod{8}$, $x \equiv 5 \pmod{8}$ e $x \equiv 7 \pmod{8}$.

L'equazione $4 \cdot x \equiv 6 \pmod{8}$ non ammette soluzioni perché $d = (4, 8) = 4$ e 4 non divide 6.

L'ultima equazione, $57 \cdot x \equiv 12 \pmod{510}$, ammette soluzioni perché $d = (57, 510) = 3$ divide 12. Il numero di soluzioni è 3. Questa volta costruiremo le soluzioni attraverso il metodo generale:

$$57 \cdot x \equiv 12 \pmod{510} \iff 57 \cdot x - 510 \cdot y = 12.$$

Poiché $57 \cdot x - 510 \cdot y = 12 \iff 19 \cdot x - 170 \cdot y = 4$ e $(19, 170) = 1$, applicando l'algoritmo di Euclide possiamo trovare una soluzione particolare dell'equazione $19 \cdot x - 170 \cdot y = 1$, e poi, moltiplicando per 4, si ottiene una soluzione dell'equazione $19 \cdot x - 170 \cdot y = 4$. Siccome

$$170 = 19 \cdot 8 + 18$$

$$19 = 18 \cdot 1 + 1$$

troviamo 1 come combinazione lineare, a coefficienti interi, di 19 e 170.

$$1 = 19 - 18 = 19 - (170 - 19 \cdot 8) = 19 \cdot 9 - 170 \cdot 1$$

$$19 \cdot 9 - 170 \cdot 1 = 1 \mid \cdot 4 \iff 19 \cdot 36 - 170 \cdot 4 = 4.$$

Quindi, una soluzione dell'equazione $19 \cdot x - 170 \cdot y = 4$ sarà $x_0 = 36,\ \ y_0 = 4$.

Le tre soluzioni dell'equazione $57 \cdot x \equiv 12 \pmod{510}$ sono $x_0,\ \ x_0 + \frac{510}{3},\ \ x_0 + 2 \cdot \frac{510}{3}$, ossia $36,\ 206,\ 376$. □

Osservazione. Ogni quadrato perfetto n^2, con $n \in \mathbb{Z}$, risulta congruo a 0 o a 1 modulo 4.

Infatti, se n è pari, cioè $n = 2 \cdot k$, allora $n^2 = 4 \cdot k^2 \equiv 0 \pmod{4}$; e se invece n è dispari, abbiamo $n = 2 \cdot k + 1$, e quindi $n^2 = 4\dot{k}^2 + 4 \cdot k + 1 \equiv 1 \pmod{4}$.

Osserviamo inoltre che non ogni numero intero congruo a 0 o a 1 modulo 4 è un quadrato perfetto. Per esempio, $20 \equiv 0 \pmod{4}$ e $21 \equiv 1 \pmod{4}$ e però, 20 e 21 non sono quadrati perfetti. □

Prolema 3. Una circonferenza è divisa in 360 parti uguali. Una frecia (lancetta) che percorre la circonferenza nel senso orario parte dallo zero e emmette un segnale acustico ogni 23 divisioni. Dopo quanti segnali sonori emmette un segnale, per la prima volta, nella divisione 73 ?

Soluzione. Mettendo il problema in equazione otteniamo l'equazione $23 \cdot x \equiv 73 \pmod{360}$, che è equivalente a l'equazione diofantea $23 \cdot x - 360 \cdot y = 73$. Quest'ultima equazione ammette soluzioni perché $d = (23, 360) = 1 | 73$. Applichiamo l'algoritmo di Euclide ai numeri 360 e 23:

$$360 = 23 \cdot 15 + 15$$

$$23 = 15 \cdot 1 + 8$$

$$15 = 8 \cdot 1 + 7$$

$$8 = 7 \cdot 1 + 1.$$

Separando i resti e sostituendo, a uno a uno, si ottiene $d = (23, 360) = 1 = 8 - 7 = 8 - (15 - 8) = 8 \cdot 2 - 15 = (23 - 15) \cdot 2 - 15 = 23 \cdot 2 - 15 \cdot 3 = 23 \cdot 2 - (360 - 23 \cdot 15) \cdot 3 = 23 \cdot 47 - 360 \cdot 3$. In questo modo abbiamo trovato una soluzione particolare dell'equazione $23 \cdot x - 360 \cdot y = 1$. Moltiplicando per 73 si ottiene

$$23 \cdot 47 \cdot 73 - 360 \cdot 3 \cdot 73 = 73 \iff 23 \cdot 3431 - 360 \cdot 219 = 73.$$

Le soluzioni dell'equazione sono $x = 3431 + 360 \cdot k$, $y = 219 + 23 \cdot k$, con $k \in \mathbb{Z}$. Riducendo la soluzione modulo 360 (richesta dalla condizione di minimalità) troviamo $3431 = 360 \cdot 9 + 191$. Quindi la soluzione del problema è $x = 191$. □

Problema 4. Si dimostri che esiste un numero naturale $a \in \mathbb{N}$ che è multiplo di 17 e le cui ultime quattro cifre sono 2009 e si determini il numero minimo a con queste proprietà.

Soluzione. Ogni numero a, le cui ultime quattro cifre sono 2009 è della forma $a = b \cdot 10000 + 2009$. Perciò $a \equiv 2009 \pmod{10000}$. Siccome $a = 17 \cdot k$, con $k \in \mathbb{N}^*$, risulta che a soddisfa l'equazione $17 \cdot x \equiv 2009 \pmod{10000}$, che è equivalente all' equazione diofantea $17 \cdot x - 10000 \cdot y = 2009$. Per quanto detto sopra, quest' ultima equazione ammette soluzioni perché $d = (17, 10000) = 1$ divide il termine noto 2009. Applichiamo l'algoritmo di Euclide per trovare $d = 1$ come combinazione lineare a coefficienti interi di 17 e 10000:

$$10000 = 17 \cdot 588 + 4,$$

$$17 = 4 \cdot 4 + 1.$$

Separando i resti e sostituendo otteniamo $1 = 17 - 4 \cdot 4 = 17 - 4 \cdot (10000 - 17 \cdot 588) = 17 \cdot (4 \cdot 588 + 1) - 10000 \cdot 4 = 17 \cdot 2353 - 10000 \cdot 4)$ e quindi $17 \cdot 2353 - 10000 \cdot 4 = 1$. Moltiplicando questa uguaglianza per 2009 si ha

$$17 \cdot 4727177 - 10000 \cdot 8036 = 2009 \iff 17 \cdot 7177 + 10000 \cdot (-8036 + 17 \cdot 472) = 2009.$$

Abbiamo ottenuto una soluzione del problema, $a = 17 \cdot 7177 = 122009$, ma non on sappiamo ancora se questa soluzione ha anche la proprietà di minimalità. A questo punto dobbiamo ricorrere al seguente fatto teorico: l'equazione $17 \cdot x \equiv 2009 \pmod{10000}$ ammette una soluzione unica in R_{10000} dato che 17 è primo con 10000. Perciò $x = 7177 \in R_{10000}$ ci fornisce il numero minimo $a = 17 \cdot 7177 = 122009$ che soddisfa le condizioni del problema. □

Problema 5. Si dimostri che la successione dei numeri 11, 111, 1111, ... non contiene quadrati perfetti.

Soluzione. Comme abbiamo osservato sopra, ogni quadrato perfetto, n^2, con $n \in \mathbb{Z}$, è congruo a 0 o a 1 modulo 4. Perciò basta considerare i resti modulo 4. Abbiamo: $11 \equiv 3 \pmod{4}$ e ogni altro termine $111 \cdots 11$ che è ha m cifre di 1, con $m \geq 3$, si può scrivere $111 \cdots 100 + 11 \equiv 3 \pmod{4}$ poiché $100 \equiv 0 \pmod{4}$. □

Teorema 7 (Il teorema cinese dei resti). *Siano m e n due numeri naturali ≥ 2 primi tra di loro. Per ogni due resti $r, s \in \mathbb{N}$ modulo m e n rispettivamente (quindi $0 \leq r < m$ e $0 \leq s < n$), esiste e si può determinare effettivamente un numero naturale a che soddisfa le seguenti condizioni $a \equiv r \pmod{m}$ e $a \equiv s \pmod{n}$.*

Dimostrazione. Il numero a deve avere il resto per la divisione con m uguale a r e il resto per la divisione con n uguale a s. Dal punto di vista insiemistico il teorema può essere riformulato dicendo che a apartiene all'intersezione

$$\{m \cdot y + r |\ y \in \mathbb{Z}\} \cap \{n \cdot z + s |\ z \in \mathbb{Z}\}.$$

Ogni soluzione del sistema

$$\begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases}$$

è anche soluzione del sistema di equazioni diofantee

$$\begin{cases} x = m \cdot y + r \\ x = n \cdot z + s, \end{cases}$$

da cui otteniamo l'equazione diofantea (in y e in z)

$$m \cdot y - n \cdot z = s - r. \tag{2}$$

Dalle ipotesi risulta che $d = (m, n) = 1$, e siccome 1 divide $s - r$, sappiamo che l'equazione (2) ammette soluzioni. Sia $(y_0,\ z_0)$, una soluzione particolare dell' equazione (2) (determinata eventualmente applicando l'algoritmo di Euclide ai numeri m e n). Le soluzioni generali dell'equazione (2) sono della forma

$$\begin{cases} y = y_0 + m \cdot k \\ z = z_0 + n \cdot k \\ k \in \mathbb{Z}. \end{cases}$$

Sostituendo queste soluzioni in $x = m \cdot y + r = n \cdot z + s$ troviamo

$$a = x = m \cdot n \cdot k + m \cdot y_0 + r = m \cdot n \cdot k + n \cdot z_0 + s,$$

dove $k \in \mathbb{Z}$ e $m \cdot y_0 - n \cdot z_0 = s - r$. □

Applicazioni.

1) Si determinino le ultime due cifre del numero 2^{9261}.

Soluzione. Determinare le ultime due cifre del numero 2^{9261} equivale a calcolare 2^{9261} modulo 100, ed e proprio questo che cercheremo a fare. Abbiamo $100 = 25 \cdot 4$. Perciò calcoliamo i resti nella divisione di 2^{9261} per 25 e, ripettivamente, per 4, cioè 2^{9261} modulo 25 e 2^{9261} modulo 4.

Poiché $9261 = 3^3 \cdot 7^3$ e

$$2^{3\cdot 7} \equiv (2^7)^3 \pmod{25} \equiv 128^3 \pmod{25} \equiv 3^3 \pmod{25} \equiv 27 \pmod{25} \equiv 2 \pmod{25},$$

otteniamo

$$2^{3^3\cdot 7^3} = (2^{3\cdot 7})^{3^2\cdot 7^2} \pmod{25} \equiv 2^{3^2\cdot 7^2} \pmod{25} \equiv (2^{3\cdot 7})^{3\cdot 7} \pmod{25} \equiv 2^{3\cdot 7} \equiv 2 \pmod{25}.$$

Inoltre, $2^{9261} \equiv 0 \pmod{4}$. Abbiamo

$$\begin{cases} 2^{9261} \equiv 2 \pmod{25} \\ 2^{9261} \equiv 0 \pmod{4} \end{cases} \iff \begin{cases} 2^{9261} = 25 \cdot y + 2 \\ 2^{9261} = 4 \cdot z. \end{cases}$$

Ora siamo in grado di applicare il Teorema cinese dei resti, con

$$a = 2^{9261},\ m = 25,\ n = 4,\ (25, 4) = 1,\ r = 2,\ s = 0.$$

Ricerchiamo una soluzione particolare dell'equazione

$$25 \cdot y - 4 \cdot z = 2. \tag{3}$$

Moltiplicando l'uguaglianza $25 = 4 \cdot 6 + 1$ per 2 otteniamo $25 \cdot 2 - 4 \cdot 12 = 2$. Quindi, le soluzioni generali dell'equazione (3) sono:

$$\begin{cases} y = 4 \cdot k + 2 \\ z = 25 \cdot k + 12 \\ k \in \mathbb{Z}. \end{cases}$$

Sostituendo, si ottiene $2^{9261} = 25 \cdot y + 2 = 25 \cdot (4 \cdot k + 2) + 2 = 100 \cdot k + 52$. In conclusione, le ultime due cifre di 2^{9261} sono 52. □

Definizione 9 (L' indicatore di Eulero). *Sia n un numero naturale, non nullo. Il numero di elementi dell'insieme*

$$U_n = \{k \mid 1 \leq k < n, (k, n) = 1\}$$

si chiama indicatore di Eulero del numero n *, e si denota con $\varphi(n)$. In altre parole, $\varphi(n)$ rappresenta il numero di numeri naturali compresi fra 1 e n, che sono primi con n.*

Ricordiamo che gli elementi dell'insieme U_n sono proprio gli elementi invetibili di $R_n = \{0, 1, 2, \ldots, n-1\}$.

Esempi. • $\varphi(4) = 2$, perché il cardinale dell'insieme $U_4 = \{1, 3\}$ è 2.
• $\varphi(5) = 4$, perché il cardinale dell'insieme $U_5 = \{1, 2, 3, 4\}$ è 4.
• $\varphi(10) = 4$, perché il cardinale dell'insieme $U_{10} = \{1, 3, 7, 9\}$ è 4.

Proposizione 5. 1) *Se p è un numero naturale primo allora $\varphi(p) = p - 1$. Più generalmente, se p è un numero naturale primo e n è un numero naturale > 0, allora $\varphi(p^n) = p^n - p^{n-1}$.*
2) *Se p e q sono due numeri naturali, primi e distinti, e m, n sono numeri naturali, allora*

$$\varphi(p^m \cdot q^n) = (p^m - p^{m-1}) \cdot (q^n - q^{n-1}) = \varphi(p^m) \cdot \varphi(q^n).$$

Più generalmente, se $p_1, p_2, \ldots, p_n$ sono n numeri naturali primi, a due a due distinti, e $m_1, m_2, \ldots, m_n$ sono numeri naturali arbitrari, allora

$$\varphi(p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}) = \varphi(p_1^{m_1}) \cdot \varphi(p_2^{m_2}) \cdots \varphi(p_n^{m_n}) =$$
$$= (p_1^{m_1} - p_1^{m_1-1}) \cdot (p_2^{m_2} - p_2^{m_2-1}) \cdots (p_n^{m_n} - p_n^{m_n-1}).$$

3) *Se a e b sono due numeri naturali non nulli e primi tra di loro, allora $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*

Dimostrazione. 1) Se $p \geq 2$ è numero primo allora tutti i numeri compresi tra 1 e $p-1$ sono primi con p. Perciò $U_p = \{1, 2, 3, \ldots, p-1\}$ e quindi $\varphi(p) = p-1$. Calcoliamo adesso $\varphi(p^n)$: si osserva che un numero $k \in \{1, 2, 3, \ldots, p^n\}$, non è primo con p^n se nella sua scomposizione a fattori compare p, cioè è della forma $k = m \cdot p$. Dalla condizione $1 \leq k \leq p^n$, equivalente a $1 \leq m \cdot p \leq p^n \iff 1 \leq m \leq p^{n-1}$, risulta che esistono p^{n-1} numeri compresi tra 1 e p^n che non sono primi con p^n. Ne risulta che l'insieme

$$U_p^n = \{1, 2, 3 \ \ldots \ , p^n\} - \{k \,|1 \leq k \leq p^n, \ (k, p^n) \neq 1\}$$

contiene $p^n - p^{n-1}$ elementi e quindi $\varphi(p^n) = p^n - p^{n-1}$.

2) Poniamo $A = \{x \in \mathbb{N} \,|1 \leq x \leq p^m \cdot q^n, \ (x, p^m) \neq 1\}$ e $B = \{x \in \mathbb{N} \,|1 \leq x \leq p^m \cdot q^n, \ (x, q^n) \neq 1\}$. Poiché p è primo, la condizione $(x, p^m) \neq 1$ equivale alla condizione $x = k \cdot p$, e quindi $1 \leq k \cdot p \leq p^m \cdot q^n$ implica $1 \leq k \leq p^{m-1} \cdot q^n$. Di conseguenza, l'insieme A contiene $p^{m-1} \cdot q^n$ elementi. Nello stesso modo (scambiando p con q), l'insieme B contiene $p^m \cdot q^{n-1}$ elemente. Poiché i numeri primi p e q sono distinti, ogni numero x è primo col prodotto $p^m \cdot q^n$, se e solo se x è primo sia con p sia con q, cioè $(x, p) = 1$ e $(x, q) = 1$. Per questo $A \cap B = \{x \,|1 \leq x \leq p^m \cdot q^n, \ x = k \cdot p \cdot q\}$ e contiene $p^{m-1} \cdot q^{n-1}$ elementi.

Ribbadiamo che $\varphi(p^m \cdot q^n)$ è il cardinale di $R_{p^m \cdot q^n} - [A \cup B]$.

Indicando con $|X|$, il numero di elementi di un qualunque insieme X, è ben nota uguaglianza

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Nelle condizioni della proposizione abbiamo

$$|A \cup B| = |A| + |B| - |A \cap B| = p^{m-1} \cdot q^n + p^m \cdot q^{n-1} - p^{m-1} \cdot q^{n-1}.$$

Ne segue

$$\varphi(p^m \cdot q^n) = |R_{p^m \cdot q^n} - [A \cup B]| = p^m \cdot q^n - |A \cup B| = p^m \cdot q^n - p^{m-1} \cdot q^n - p^m \cdot q^{n-1} + p^{m-1} \cdot q^{n-1} =$$

$$= (p^m - p^{m-1})(q^n - q^{n-1}) = \varphi(p^m) \cdot \varphi(q^n).$$

La dimostrazione della formula nel caso generale, utilizza il metodo dell'induzione matematica e il principio dell'inclusione e esclusione. Il principio dell'inclusione e esclusione rappresenta la generalisazione della formula $|A \cup B| = |A| + |B| - |A \cap B|$. Per esempio, considerando tre insiemi A, B, C, vale la relazione

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Usando la decomposizione in fattori primi di un numero naturale e il punto 2) della proposizione si dimostra che la funzione φ commuta con il prodotto dei numeri primi tra di loro. □

Commento. Siano $m, n \in \mathbb{N}$ due numeri naturali primi tra di loro. La formula $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, può essere interpretata nel contesto della teoria delle probabilità nel modo seguente: La probabilità che un numero naturale, compreso fra 1 e $m \cdot n$ sia relativamente primo con il prodotto $m \cdot n$ (cioè $\frac{\varphi(m \cdot n)}{m \cdot n}$), è uguale al prodotto della probabilità che il numero sia primo con m e la probabilità che il numero sia primo con n (cioè $\frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n}$.)

Esempi.

1) $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$,

2) $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$,

3) $\varphi(128) = \varphi(2^7) = 2^7 - 2^6 = 64$,

4) $\varphi(1024) = \varphi(2^{10}) = 2^{10} - 2^9 = 512$,

5) $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$,

6) $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$,

7) $\varphi(2009) = \varphi(7^2 \cdot 41) = \varphi(7^2) \cdot \varphi(41) = (7^2 - 7) \cdot (40) = 1680$.

È utile ricordare la seguente proprietà (che sarà utilizzata nelle dimostrazioni che seguirano): se due numeri naturali non nulli, a e n, sono primi tra di loro, allora per ogni x, y tali che $a \cdot x \equiv a \cdot y \pmod{n}$ risulta $x \equiv y \pmod{n}$. Ne diamo un' altra dimostrazione di questa proprietà. Dalla condizione $a \cdot x \equiv a \cdot y \pmod{n}$ si ottiene $a \cdot x - a \cdot y = k \cdot n,\ k \in \mathbb{Z} \iff a \cdot (x - y) = k \cdot n$ e quindi n divide il prodotto $a \cdot (x - y)$. Siccome n è primo con a risulta che n divide $x - y$, e quindi $x \equiv y \pmod{n}$.

Teorema 8 (Il piccolo teorema di Fermat). *Sia p un numero naturale primo. Allora per ogni numero naturale a si ha $a^p \equiv a \pmod{p}$.*

Dimostrazione. Ne diamo due dimostrazioni utilizzando metodi ben diversi.

Prima dimostrazione. Procediamo per l'induzione secondo a. Se $a = 0$ allora $0^p \equiv 0 \pmod{p}$. Se $a = 1$ allora $1^p \equiv 1 \pmod{p}$. Supponiamo che per un a fissato valga $a^p \equiv a \pmod{p}$. Bisogna dimostrare che $(a+1)^p \equiv a+1 \pmod{p}$. Nello sviluppo del binomio $(a+1)^p$ compaiono i coefficienti binomiali C_p^k. Per $1 \leq k \leq p-1$ i coefficienti binomiali sono congruenti allo zero perché p è un numero primo. Di conseguenza

$$(a+1)^p = a^p + C_p^1 \cdot a^{p-1} + C_p^2 \cdot a^{p-2} + \cdots + C_p^{p-2} \cdot a^2 + C_p^{p-1} \cdot a + 1 \equiv a^p + 1 (\mathrm{mod}\, p) \equiv a + 1 (\mathrm{mod}\, p).$$

Seconda dimostrazione. Osserviamo che possiamo suppore che $a \in R_p^* = \{1, 2, 3, \ldots, p-1\}$. Infatti, se $a = p \cdot k + r$, con $r \in R_p$, allora $a = p \cdot k + r \equiv r \pmod{p}$, e quindi $a^p \equiv r^p \pmod{p}$. Poiché ogni $a \in \{1, 2, \ldots,\ p-1\}$ è primo con p, a e quindi invertibile in R_p. Di conseguenza, per ogni $x, y \in \mathbb{Z}$ tali che $a \cdot x \equiv a \cdot y \pmod{p}$ risulta $x \equiv y \pmod{p}$. Equivalentemente, per ogni $x, y \in R_p^*$, con $x \neq y$, abbiamo $a \cdot x \not\equiv a \cdot y \pmod{p}$. Ne segue che l'insieme $\{a \cdot 1,\ a \cdot 2,\ \ldots\ , a \cdot (p-1)\}$ contiene $p-1$ elementi, equivalenti ai $p-1$ resti modulo p, cioè $\{1, 2, \ldots, p-1\}$. Per la commutatività della moltiplicazione otteniamo

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \iff$$
$$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv (1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p} \iff a^{p-1} \equiv 1 \pmod{p}.$$

La semplificazione per $(p-1)!$ è stata consentita dal fatto che $(p-1)!$ è primo con p. □

È possibile generalizare il piccolo terema di Fermat considerando al posto del numero primo p, un numero naturale $n \in \mathbb{N}^*$ primo con a.

Teorema 9 (Teorema di Eulero). *Siano $a, n \geq 2$ due numeri naturali primi tra di loro. Allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Dimostrazione. Nell'insieme dei resti modulo n, $R_n = \{0, 1, 2,\ \ldots\ , n-1\}$ esistono esatamente $\varphi(n)$ resti primi con n. Sia $U_n = \{r_1, r_2,\ \ldots\ , r_{\varphi(n)}\}$ l'insieme dei resti modulo n, primi con n. Consideriamo due resti r_i, r_j tali che $a \cdot r_i \equiv a \cdot r_j \pmod{n}$. Dalla condizione che a è primo con n, risulta $r_i \equiv r_j \pmod{n}$. Riformulando, possiamo dire che se $r_i \not\equiv r_j \pmod{n}$ allora $a \cdot r_i \not\equiv a \cdot r_j \pmod{n}$. Di conseguenza si ottengono le congruenze

$$a \cdot r_1 \equiv r_{i_1} \pmod{n}$$
$$a \cdot r_2 \equiv r_{i_2} \pmod{n}$$
$$a \cdot r_3 \equiv r_{i_3} \pmod{n}$$

. . . . . .

$$a \cdot r_{\varphi(n)} \equiv r_{i_{\varphi(n)}} \pmod{n}.$$

Moltiplicandole a membro a membro otteniamo:

$$a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)} \equiv r_{i_1} \cdot r_{i_2} \cdot \ \ldots \ \cdot r_{\varphi(n)} \pmod{n} \tag{4}$$

Notiamo che ogni due resti nel secondo membro sono distinti. Perciò otteniamo

$$\{r_{i_1}, r_{i_2}, r_{i_3}, \ \ldots \ , r_{i_{\varphi(n)}}\} = \{r_1, r_2, r_3, \ \ldots \ , r_{\varphi(n)}\}.$$

Inoltre, il prodotto $r_{i_1} \cdot r_{i_2} \cdot \ \ldots \ \cdot r_{\varphi(n)}$ coincide col prodotto $r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)}$ (perché la moltiplicazione è commutativa). Allora l'equivalenza (4) diventa:

$$a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)} \pmod{n}.$$

Ogni resto da $U_n = \{r_1, r_2, \ \ldots \ , r_{\varphi(n)}\}$ è primo con n. Ne segue che anche il prodotto $r_1 \cdot r_2 \cdot r_3 \cdots r_{\varphi(n)}$ è primo con n, e quindi possiamo semplificare per esso nell' ultima congruenza e otteniamo

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

ciò che conclude la dimostrazione. □

Esempi. 1) $3^{\varphi(100)} = 3^{40} \equiv 1 \pmod{100}$.

2) $2^{\varphi(2009)} = 2^{42 \cdot 40} = 2^{1680} \equiv 1 \pmod{2009}$ perché $2009 = 7^2 \cdot 41$, e quindi $\varphi(2009) = \varphi(7^2) \cdot (41) = (7^2 - 7) \cdot (40) = 42 \cdot 40 = 1680$. In altre parole, il resto nella divisione di 2^{1680} per 2009 è uguale a 1.

3) $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$.

Proposizione 6. *Sia p un numero naturale primo. L'equazione $x^2 \equiv 1 \pmod{p}$ ammette esatamente due soluzioni $x \equiv 1 \pmod{p}$ e $x \equiv (p-1) \pmod{p}$. In altre parole 1 e $p-1$ sono gli unici numeri da $R_p = \{0, 1, 2, \ \ldots \ , p-1\}$, i cui inversi coincidono con loro stessi.*

Dimostrazione. $x^2 \equiv 1 \pmod{p} \iff (x-1) \cdot (x+1) \equiv 1 \pmod{p} \iff p|(x-1) \cdot (x+1)$. Dalla definizione sappiamo che ogni numero primo che divide in prodotto, divide almeno uno dei fattori. Perciò, $p|(x-1) \cdot (x+1)$ implica $p|(x-1)$ sau $p|(p+1)$. Ne risulta

$$x - 1 = k \cdot p, \ \ k \in \mathbb{Z} \iff x = 1 + k \cdot p \iff x \equiv 1 \pmod{p}$$

o ancora,

$$x + 1 = k \cdot p, \ \ k \in \mathbb{Z} \iff x = -1 + k \cdot p = p - 1 + (k-1) \cdot p \iff x \equiv (p-1) \pmod{p}. \quad \square$$

Ora dimostriamo un bel teorema che è alche utile nelle applicazioni.

Teorema 9 (Teorema di Wilson). *Sia p un numero naturale primo. Allora $(p-1)! + 1 \equiv 0 \pmod{p}$.*

Dimostrazione. Ne diamo due dimostrazioni.

Prima dimostrazione. Abbiamo $(p-1)! = 1 \cdot 2 \cdots (p-1)$. Il teorema si verifica banalmente per $p = 2$ e per $p = 3$. Perciò possiamo supporre che $p \geq 5$. Ciascuno dei numeri $1, 2, 3, \ldots, p-1$ è primo con p, e perciò è invertibile. Come nella Proposizione 6 abbiamo dimostrato che l'inverso di 1 è 1 e l'inverso di $p-1$ è $p-1$ (e che 1 e $p-1$ sono gli unici con questa proprietà), per ogni $a \in \{2, 3, \ldots, (p-2)\}$ esiste $b \in \{2, 3, \ldots, (p-2)\}$, $b \neq a$, tale che $a \cdot b \equiv 1 \pmod{p}$. Nel prodotto $2 \cdot 3 \cdot \ldots \cdot (p-2)$, raggruppando ogni numero diverso da 1 e $p-1$, con il suo inverso, si ottiene:

$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$. Quindi $1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$. In conclusione $(p-1)! + 1 \equiv -1 + 1 \pmod{p} \equiv 0 \pmod{p}$. □

Seconda dimostrazione. Questa dimostrazione è basata sulle proprietà elementari dei polinomi. Consideriamo il polinomio $P(X) = X^{p-1} - 1$ a coefficienti in R_p, con p è un numero primo. Ogni $x \in U(R_p) = \{1, 2, 3, \ldots, p-1\}$ è radice del polinomio $P(X)$ perche $x^{\varphi(p)} = x^{p-1} \equiv 1 \pmod{p}$ e quindi $x^{p-1} - 1 \equiv 0 \pmod{p}$. In questo caso, l'ultima formula di Viète diventa $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv (-1)^{p-1} \cdot (-1) \pmod{p} \equiv (-1) \pmod{p}$, cioè $(p-1)! + 1 \equiv 0 \pmod{p}$. □

Applicazioni.

1) Si dimostri che per ogni due numeri naturali $a, b \in \mathbb{N}^*$ positivi, che primi tra di loro, il numero $(a^6 + b^6 - 1)(a^6 + b^6 - 2)$ è divisibile per 252.

Soluzione. Notiamo che $252 = 4 \cdot 7 \cdot 9$. Dalla definizione della relazione di congruenza risulta

$$252 | (a^6 + b^6 - 1)(a^6 + b^6 - 2) \iff (a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{252}$$

$$\iff \quad (a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{(4 \cdot 7 \cdot 9)}.$$

I numeri $4, 7, 9$ sono primi tra di loro, e quindi il problema si riduce a provare il fatti seguenti:

$$(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{4},\ (a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{7} \text{ e}$$

$$(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{9}.$$

Congruenza modulo 4: se $a \equiv 0 \pmod{2}$ e $b \not\equiv 0 \pmod{2}$ (cioè a è pari e b è dispari), allora $a^2 \equiv 0 \pmod{4}$ e $b^2 \equiv 1 \pmod{4}$. Risulta $a^6 + b^6 - 1 \equiv 0 \pmod{4}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{4}$. Se $a \not\equiv 0 \pmod{2}$ e $b \not\equiv 0 \pmod{2}$ (cioè a è dispari e b este dispari), allora $a^2 \equiv 1 \pmod{4}$ e $b^2 \equiv 1 \pmod{4}$. Risulta $a^6 + b^6 - 2 \equiv 0 \pmod{4}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{4}$.

Congruenza modulo 7: se x è primo con 7 allora $x^{\varphi(7)} = x^6 \equiv 1 \pmod{7}$. Se $a \equiv 0 \pmod{7}$ e $b \not\equiv 0 \pmod{7}$ (cioè se a è multiplo di 7 e b non è multiplo di 7), allora $a^6 \equiv 0 \pmod{7}$ e $b^6 \equiv 1 \pmod{7}$. Risulta $a^6 + b^6 - 1 \equiv 0 \pmod{7}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{7}$.

Se $a \not\equiv 0 \pmod{7}$ e $b \not\equiv 0 \pmod{7}$ (cioè se a non è multiplo di 7 e b non è este multiplo di 7), allora $a^6 \equiv 1 \pmod{7}$ e $b^6 \equiv 1 \pmod{7}$. Risulta $a^6 + b^6 - 2 \equiv 0 \pmod{7}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{7}$.

Congruenza modulo 9: se x è primo con 9 allora $x^{\varphi(9)} = x^6 \equiv 1 \pmod{9}$. Se $a \equiv 0 \pmod{9}$ e $b \not\equiv 0 \pmod{9}$ (cioè se a è multiplo di 9 e b non è multiplo de 9), allora $a^6 \equiv 0 \pmod{9}$ e $b^6 \equiv 1 \pmod{9}$. Risulta $a^6 + b^6 - 1 \equiv 0 \pmod{9}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{9}$.

Se $a \not\equiv 0 \pmod{9}$ e $b \not\equiv 0 \pmod{9}$ (cioè se a non è multiplo di 9 e b non è multiplo di 9), allora $a^6 \equiv 1 \pmod{9}$ e $b^6 \equiv 1 \pmod{9}$. Risulta $a^6 + b^6 - 2 \equiv 0 \pmod{9}$ e quindi $(a^6 + b^6 - 1)(a^6 + b^6 - 2) \equiv 0 \pmod{9}$. □

2) Si determini il minimo numero naturale $n \in \mathbb{N}^*$ tale che $2^n \equiv 1 \pmod{47}$.

Soluzione. Osserviamo che 47 è un numero primo e 2 è primo con 47. Per il teorema di Eulero abbiamo $2^{\varphi(47)} = 2^{46} \equiv 1 \pmod{47}$. Affermiamo che ogni numero $n \in \mathbb{N}^*$ con $n \leq 46$ che soddisfa la congruenza $2^n \equiv 1 \pmod{47}$, è un divisore di 46. Infatti, sia $n \in \mathbb{N}^*$, con $n \leq 46$ minimo tale che $2^n \equiv 1 \pmod{47}$. Dividendo 46 per n col resto, otteniamo $46 = n \cdot k + r,\ 0 \leq r < n$; esponenziando in base 2, si ricava $1 \equiv 2^{46} \pmod{47} \equiv (2^{n \cdot k + r}) \pmod{47} \equiv [(2^n)^k \cdot 2^r] \equiv [1^k \cdot 2^r] \pmod{47} \equiv 2^r$, e quindi $2^r \equiv 1 \pmod{47}$ con $0 \leq r < n$. Dalla minimalità di n risulta che $r = 0$ (altrimenti n non sarebbe il minimo con la proprietà $2^n \equiv 1 \pmod{47}$). Perciò, $46 = n \cdot k$, con $k \in \mathbb{Z}$, e quindi n divide 46.

Ora si sceglie n come il minimo divisore di 46 che soddisfa la condizione $2^n \equiv 1 \pmod{47}$. Bisogna verificare che: $2^1 = 2 \equiv 2 \pmod{47}$, $2^2 = 4 \equiv 4 \pmod{47}$, $2^{23} \equiv [(2^{10})^2 \cdot 2^3] \pmod{47} \equiv$

$[(1024)^2 \cdot 8] \pmod{47} \equiv [(47 \cdot 21 + 37)^2 \cdot 8] \pmod{47} \equiv (-10)^2 \cdot 8 \pmod{47} \equiv 46 \pmod{47}$. L'unica possibilità è $n = 46$, che in questo caso rappresenta $\varphi(47)$. □

Osservazione. Possiamo chiederci la seguente domanda: vale sempre la conclusione dell'esercizio precedente, nel senso che $n = \varphi(p)$, con p primo, è l'esponente minimo per il quale $2^n \equiv 1 \pmod{47}$? La risposta è negativa come ci mostra il seguente esempio. Se consideriamo $p = 7$, invece di 47, l'esponente minimo che soddisfa $2^n \equiv 1 \pmod{7}$ è $n = 3$, poiché $2^3 \equiv 1 \pmod{7}$; inoltre, 3 è un divisore di $\varphi(7) = 6$.

Sia $n \in \mathbb{N}^*$ fissato e a un numero naturale, primo con n. Per il teorema di Eulero, ottiene $a^{\varphi(n)} \equiv 1 \pmod{n}$. In generale $\varphi(n)$ non è necessariamente il minimo esponente $x \in \mathbb{N}^*$ che soddisfa la condizione $a^x \equiv 1 \pmod{n}$. Quello che si può solo dire è che il minimo x che soddisfa $a^x \equiv 1 \pmod{n}$ è un divisore di $\varphi(n)$. La dimostrazione segue dalla soluzione dell' esercizio 2). Sia $m \in \mathbb{N}^*$, in numero naturale non nullo minimo per cui vale $a^m \equiv 1 \pmod{n}$. Dal teorema di divisione col resto otteniamo $\varphi(n) = m \cdot k + r,\ k \in \mathbb{Z},\ 0 \leq r < m$. Sostituendo, si ricava

$$a^{\varphi(n)} = a^{m \cdot k + r} = [a^m]^k \cdot a^r \iff 1 \equiv a^r \pmod{n}.$$

Per la minimalità di m risulta $r = 0$, e quindi m divide $\varphi(n)$. □

3) Siano $m, n \in \mathbb{N}$ tali che $1 \leq m < n$ e e tali che le ultime tre cifre del numero 1978^n coincidono con le ultime tre cifre del numero 1978^m. Si determinino m e n che godono le proprietà precedenti e, inoltre, tale che la somma $m + n$ sia minima.

Soluzione. Le ultime tre cifre di due numeri coincidono quando la loro differenza si divide per 1000, cioè, quendo i due numeri sono congruenti modulo 1000. Perciò possiamo riformulare il problema nel modio seguete: si determinino $m, n \in \mathbb{N},\ 1 \leq m < n$, tali che $1978^m \equiv 1978^n \pmod{1000}$ e tali che la somma $m + n$ sia minima.

Abbiamo $1978^n - 1978^m = 1978^m \cdot [1978^{n-m} - 1] = 2^m \cdot 989^m \cdot [1978^{n-m} - 1]$. Inoltre, $1000 = 2^3 \cdot 5^3$. Siccome i numeri 2^3 e 5^3 sono primi tra di loro, bisohna imporre le seguenti condizioni:

$$2^3 | (1978^n - 1978^m) \text{ e } 5^3 | (1978^n - 1978^m) \iff$$

$$\begin{cases} 1978^n - 1978^m \equiv 0 \pmod{2^3} \\ 1978^n - 1978^m \equiv 0 \pmod{5^3}. \end{cases}$$

Il numero $989^m \cdot (1978^{n-m} - 1)$ è dispari, perciò il fatto che 2^3 divide $1978^n - 1978^m$ significa che $2^3 | 2^m$, da cui otteniamo $m \geq 3$.

La somma $n + m = (n - m) + 2 \cdot m \geq (n - m) + 6$ diventa minima per $m = 3$ e $n - 3$ minimo. (Infatti per $m > 3 \implies n + m > n + 3$.)

Ora sfruttiamo la condizione che $5^3 | (1978^n - 1978^m) = 2^m \cdot 989^m \cdot (1978^{n-m} - 1)$; poiché 5 è primo con 2 e con 989, l' ultima condizione equivale alla seguente

$$5^3 | (1978^{n-3} - 1) \iff 1978^{n-3} \equiv 1 \pmod{125}.$$

Dal teorema di Eulero ($(1978, 125) = 1$) si ottiene

$$1978^{\varphi(125)} \equiv 1 \pmod{125} \iff 1978^{100} \equiv 1 \pmod{125}.$$

Sia k l'esponente non nullo minimo, che soddisfa $1978^k \equiv 1 \pmod{125}$. Affermiamo che $k | 100$. Infatti, se $100 = k \cdot l + r$ con $l, r \in \mathbb{Z},\ 0 \leq r < k$ allora

$$1 \equiv 1978^k \pmod{125} \equiv (1978^k)^l \cdot 1978^r \pmod{125} \equiv 1978^r \pmod{125},$$

e per la proprietatà di minimalità di k, risulta che $r = 0$ e quindi $k | 100$, ossia $k \in \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$. Siccome $k = n - 3 > 0$ si trova $k \geq 4$. Osserviamo che

$$1978^k \equiv 1 \pmod{125} \implies 1978^k \equiv 1 \pmod{5},$$

e poiché $1978 \equiv 3 \pmod 5$, l' ultima condizione equivale alle seguenti congruenze

$$3^k \equiv 1 \pmod 5 \text{ e } 3^4 \equiv 1 \pmod 5.$$

Dalla proprietatà di minimalità risulta che $4|k$ (perché $3^1, 3^2, 3^3 \not\equiv 1 \pmod 5$). Quindi $k \in \{4, 20, 100\}$. Allora abbiamo:

$$1978^4 \equiv (2000 - 22) \pmod{125} \equiv 22^4 \pmod{125} \equiv \pmod{125} \not\equiv 1 \pmod{125},$$

$$1978^{20} \equiv 6^5 \pmod{125} \equiv 26 \pmod{125} \not\equiv 1 \pmod{125}.$$

Di conseguenza $n - 3 = k = 100$, e quindi $n = 103, m = 3, n + m = 106$. □

4) Sia D un determinante di ordine 36 le cui entrate sono $a_{ij} = i \cdot j$, $i, j = 1, \ldots, 36$. Si dimostri che il modulo di ogni termine nel suo svolgimento è congruo a 1 modulo 37.

Soluzione. Ogni termine dello svolgimento di un determinante di ordine n con le entrate a_{ij} è della forma

$$(-1)^{\varepsilon(\sigma)} a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot a_{3\sigma(3)} \cdots a_{n\sigma(n)}.$$

Per ogni permutazione σ gli insiemi $\{\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)\}$ e $\{1, 2, 3, \ldots, n\}$ coincidono. Ne segue che $\sigma(1) \cdot \sigma(2) \cdot \sigma(3) \cdots \sigma(n) = 1 \cdot 2 \cdot 3 \cdots n = n!$. Nel nostro caso,

$$(-1)^{\varepsilon(\sigma)} a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot a_{3\sigma(3)} \cdots a_{36,\sigma(36)} =$$

$$= (-1)^{\varepsilon(\sigma)} \cdot 1 \cdot \sigma(1) \cdot 2 \cdot \sigma(2) \cdot 3 \cdot \sigma(3) \cdots 36 \cdot \sigma(36) = (-1)^{\varepsilon(\sigma)} \cdot (36)! \cdot (36)! = (-1)^{\varepsilon(\sigma)} \cdot [(36)!]^2,$$

ciò che implica

$$|(-1)^{\varepsilon(\sigma)} a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot a_{3\sigma(3)} \cdots a_{36,\sigma(36)}| = [36!]^2.$$

D'altro canto, dal teorema di Wilson risulta $(37 - 1)! + 1 \equiv 0 \pmod{37}$, ossia $36! \equiv -1 \pmod{37}$, da dove finalmente otteniamo $[36!]^2 \equiv 1 \pmod{37}$.

Osservazione. Evidentemente, in questo esercizio il numero 37 può essere sostituito con un qualsiasi numero primo p. □